Intelligence and Security Committee of Parliament

Annual Report 2019–2021

Chairman:
The Rt Hon. Dr Julian Lewis MP

HC 877

Intelligence and Security Committee of Parliament

Annual Report 2019–2021

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
10 December 2021

HC 877

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

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

ISBN 978-1-5286-3040-5

E02696743 12/21

Printed on paper containing 75% recycled fibre content minimum

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

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

The Rt Hon. Dr Julian Lewis MP (Chairman)

The Rt Hon. Sir John Hayes CBE MP
The Rt Hon. Stewart Hosie MP
The Rt Hon. Dame Diana Johnson DBE MP
The Rt Hon. Kevan Jones MP

The Rt Hon. Mark Pritchard MP
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

This Report also covers the work of the previous Committee, which sat from November 2017 to November 2019.*

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),[‡] and the work of the Joint Intelligence Organisation (JIO) and the National Security Secretariat (NSS) in the Cabinet Office, Defence Intelligence (DI) in the Ministry of Defence (MoD), and Homeland Security Group (HSG) in the Home Office.[§]

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

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

The Reports can contain highly classified material, which would damage the operational capabilities of the intelligence Agencies if it were published. There is therefore a well-established

[*] The membership of the previous Committee was: The Rt Hon. Dominic Grieve QC MP (Chair), The Rt Hon. Richard Benyon MP, The Rt Hon. Caroline Flint MP, The Rt Hon. David Hanson MP, The Rt Hon. Stewart Hosie MP, The Rt Hon. the Lord Janvrin GCB GCVO QSO, The Rt Hon. Kevan Jones MP, The Most Hon. the Marquess of Lothian PC QC, and The Rt Hon. Keith Simpson MP.

[†] Throughout the Report, the term 'Intelligence Community' is used to refer to the seven organisations that the Committee oversees. The term 'Agencies' refers to MI5, SIS and GCHQ as a collective and the term 'Departments' refers to the intelligence and security parts of the MoD, Cabinet Office and the Home Office (DI, JIO, National Security Adviser (NSA), NSS and HSG) as a collective, unless specified otherwise.

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

[§] 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 formerly 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) [source: Home Office, 25 August 2021].

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 July 2019 to July 2021, in carrying out its oversight of the Intelligence Community.[1]

Membership during the period covered by this Report

2. On 5 November 2019, in line with the Justice and Security Act 2013, Members of the ISC vacated their posts upon the dissolution of Parliament prior to the December 2019 General Election.

3. The Committee was not reconstituted until 14 July 2020 – over eight months later. This delay was longer even than those after both the previous General Elections, in 2015 and 2017. Every time there is a UK election there are significant delays in the appointment of the Committee. There is no reason for any delay, which results in lengthy gaps in oversight – and in this instance unnecessarily delayed the publication of the Committee's *Russia* Report.

4. The Committee held its inaugural meeting on 15 July 2020, at which Members elected the Rt Hon. Dr Julian Lewis MP as Chairman, under the Justice and Security Act 2013.

5. On 28 August 2020, the Rt Hon. Chris Grayling MP notified the Chairman of his intent to step down from his role on the Committee. Following a consultation process, as set out in the Justice and Security Act 2013, the Rt Hon. Bob Stewart MP was nominated for membership of the Committee by the Prime Minister, and was appointed by the House of Commons on 16 September 2020.

Work programme

6. In carrying out its work, the Committee:

- held 30 full Committee meetings, including evidence sessions with Government Ministers, senior officials from across the Intelligence Community, and external experts;
- visited organisations across the Intelligence Community on five occasions;
- held bilateral discussions with the Canadian intelligence community; and
- held 17 other meetings.

7. During the period covered by this Report, the Committee concluded three Inquiries – on Russia, Northern Ireland-related terrorism (NIRT) and GCHQ accommodation procurement – completed its Annual Report for 2018–2019 and 2019–2021, and published three Statements.

8. The Committee's work has been affected by the COVID-19 pandemic with meetings having to be rescheduled on a number of occasions during periods of national lockdown (the

[1] The Committee had intended to publish an Annual Report earlier in the year; however, the Intelligence Community failed to meet the required deadlines. It therefore had to be delayed, and as a result this Report now covers a longer period than usual.

classified nature of the Committee's work means that it cannot conduct its business virtually, as Select Committees are able to). It has also been affected by significant delays in information being provided to the Committee by the Intelligence Community, as they themselves have been affected by the pandemic and have had to focus their reduced resources on the immediate national security threats.

Russia

9. The previous Committee completed its Inquiry into the threat posed by Russia in October 2019 and sent its Report to the Prime Minister on 17 October 2019, for him to confirm under the Justice and Security Act 2013 that there was no material remaining in the Report which would prejudice the discharge of the functions of the Agencies[2] – a process which by convention has taken ten working days. However, that confirmation was in this instance not received until 13 December 2019, some 43 days later, and after the Committee had been stood down for the General Election. This delay to publication was the subject of a great deal of speculation in the media, given that it meant that the Report could not be published before the General Election on 12 December. Contrary to some speculation, the delay was not due to the Committee: the Report had been sent to the Prime Minister with plenty of time to enable it to be published before the election, had confirmation been received in the usual manner.

10. The Committee's Reports must be laid by the Committee before Parliament, and therefore the *Russia* Report could not be published until both the Committee was reappointed and Parliament was sitting. The Report was finally published on 21 July 2020: the first such opportunity, despite it having been completed on 17 October the previous year.

11. The Report questioned whether the Government took its eye off the ball with regard to Russia, because of its focus on counter-terrorism. The previous Committee found that until recently the Government had badly underestimated the response required to the Russian threat and is still playing catch up. Russia is able to pose an all-encompassing security threat – which is fuelled by paranoia about the West and a desire to be seen as a resurgent great power – and, given the UK's firm stance recently against Russian aggression and the UK-led international response to the 2018 Salisbury attack, the UK is one of Russia's top Western intelligence targets.

12. The previous Committee found that Russia is a highly capable cyber actor, employing organised crime groups to supplement its cyber skills, carrying out malicious cyber activity in order to assert itself aggressively and undertaking cyber pre-positioning on other countries' Critical National Infrastructure. The Committee was therefore concerned to find no clear co-ordination between the numerous organisations across the UK Intelligence Community working on this issue, and an unnecessarily complicated wiring diagram of responsibilities amongst Ministers. Nevertheless, the Committee did welcome the Government's increasingly assertive approach when it comes to identifying, and laying blame on, the perpetrators of cyber attacks and considered that the UK should encourage other countries to adopt a similar approach to 'naming and shaming' and to work towards an international doctrine on the use of Offensive Cyber.

[2] 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 MI5, SIS and GCHQ (collectively, 'the Agencies') or of other parts of the Intelligence Community. The ISC may also, as appropriate, report to the Prime Minister.

13. The Report also considered Russia's promotion of disinformation and attempts at political influence overseas – whether through the use of social media, hack and leak operations, or its state-owned traditional media. It was this issue in particular that led to the considerable controversy surrounding the delay in publication of the Report until after the General Election. The previous Committee found that the UK is clearly a target, but that no one within Government was prepared to take responsibility for defence of the UK's democratic processes: no single organisation was prepared to accept the overall lead. The Committee questioned whether some of the organisations currently involved have the weight and access required to tackle a major hostile state threat and recommended that Homeland Security Group (formerly known as Office for Security and Counter-Terrorism – OSCT) should take the policy lead and the operational role should sit with MI5. The Report did note, however, that – as with so many other issues currently – it is the social media companies who hold the key but are failing to play their part. The Committee recommended that the Government establish a protocol with these companies to ensure that they take covert hostile state use of their platforms seriously, with agreed deadlines within which such material will be removed, and Government should 'name and shame' those which fail to act.

14. The Report considered the widespread allegations that Russia sought to influence voters in the 2016 referendum on the UK's membership of the European Union (EU): studies pointed to the preponderance of pro-Brexit or anti-EU stories on RT and Sputnik, and the use of 'bots' and 'trolls', as evidence. The previous Committee considered that the actual impact of such attempts on the result itself would be difficult – if not impossible – to assess. However, it was clear that the Government was slow to recognise the existence of the threat – only understanding it after the 'hack and leak' operation against the Democratic National Committee in the United States, when it should have been seen as early as 2014. As a result, the Government did not take action to protect the UK's process in 2016. The Committee also reported that it had not been provided with any post-referendum assessment – in stark contrast to the US response to reports of interference in the 2016 presidential election. We note that a cross-party group of MPs and Peers have now filed a legal claim against the Government for failing to produce such an assessment.

15. More broadly, the extent of Russian influence in the UK is very clear – the previous Committee found it to be 'the new normal', as successive Governments have welcomed the Russian oligarchy with open arms. As a result, there are a lot of Russians with very close links to Putin who are well integrated into the UK business, political and social scene – in 'Londongrad' in particular. Yet the previous Committee found that few, if any, questions have been asked regarding the provenance of their considerable wealth and this 'open door' approach provided ideal mechanisms by which illicit finance could be recycled through the London 'laundromat'. It is not just the oligarchs either – the arrival of Russian money has resulted in a growth industry of 'enablers': lawyers, accountants and estate agents have all played a role, wittingly or unwittingly, and formed a 'buffer' of Westerners who are de facto agents of the Russian state.

16. The previous Committee recognised the inherent tension between the Government's prosperity agenda and the need to protect national security, and that to a certain extent it was not possible to untangle it: the priority now must be to try and reduce the risk, and ensure that where hostile activity is uncovered, the proper tools exist to tackle it at source. The Committee highlighted that a number of Members of the House of Lords have business interests linked to Russia, or work directly for major Russian companies linked to the Russian state, and

recommended that such relationships be carefully scrutinised and the Code of Conduct for Members of the House of Lords, and the Register of Lords' Interests, including financial interests, be enforced – given the potential for the Russian state to exploit them.

17. On this point, we note that the House of Lords has taken very swift action. On 23 July 2020, the House of Lords Conduct Committee issued a statement saying that it had discussed the findings and recommendations in the ISC Report relating to the House of Lords and that it had commissioned work on possible changes to the Code. At its subsequent meeting on 17 September 2020, the Conduct Committee agreed to recommend to the House that Members be required to disclose earnings from work for foreign governments and for associated companies/organisations.[3] This is a very welcome development, and we commend the House for acting so promptly where concerns are raised.

18. We hope that the Government will take such positive action in response to the other recommendations in the Report – in particular in response to the call for new legislation to provide the intelligence Agencies with the tools they need to tackle the intelligence challenges posed by Russia. We understand that the Government is continuing to work on this and we expect a Bill to be produced as a matter of legislative priority in 2021.

Annual Report 2018–2019

19. In addition to the *Russia* Report, the Committee's Annual Report 2018–2019 had also been held back from publication due to the Prime Minister not having provided confirmation that it could be published before the Committee was stood down for the General Election. (The Annual Report had also been sent to the Prime Minister on 1 November 2019, and confirmation was also not received until 13 December 2019.) The Report – which summarised the work of the Committee for the period August 2018 to July 2019 – was finally published on 21 July 2020.

Northern Ireland-related terrorism (NIRT)

20. Following the reckless violence that led to the death of journalist Lyra McKee at the hands of a 'new IRA' gunman in April 2019, the previous Committee undertook an Inquiry into the threat from Northern Ireland-related terrorism. The Committee published its Report on 5 October 2020.

21. The Report made clear that the main Dissident Republican groups are resilient and retain both the intent and capability to cause serious damage. The groups appear to be continuing to recruit new members, including significant numbers of young people. The Committee therefore welcomed the Government's efforts to apply the lessons drawn from counter-terrorism work across the UK to Northern Ireland, noting that it is essential that non-national security departments with better links into the community are able to provide positive interventions if they spot early-stage involvement in terrorist groups.

22. The Report raised concerns that pursuing criminal justice outcomes remains challenging, with systemic delays and lenient sentencing, and the Committee urged the Executive and Assembly to consider urgently how criminal justice outcomes can be improved. The Report

[3] House of Lords Conduct Committee, Thursday 17 September 2020, 9th Meeting COND/19-21.

also addressed the ‘Third Direction’ case, which was then being heard in the Investigatory Powers Tribunal, and which has since led to the Covert Human Intelligence Sources (Criminal Conduct) Act, covered further below.

23. The Committee commended the efforts of MI5 and the Police Service of Northern Ireland, but cautioned that the threat requires sustained pressure and resources must be maintained.

24. On 11 February 2021, the Government published its response to the Report. The response said that the Government continues to prioritise support for efforts to ensure a safer Northern Ireland, where terrorist and paramilitary groups are less able to cause harm to communities. The response also notes two main points of progress against the recommendations and conclusions identified in the NIRT Report – the continued work of the cross-Executive ‘Tackling Paramilitarism, Criminality and Organised Crime’ programme, and the introduction of the Covert Human Intelligence Sources (Criminal Conduct) Bill on 24 September 2020.

GCHQ accommodation procurement

25. In November 2015, the then Chancellor announced[4] that the UK would establish a new “*National Cyber Centre*” in 2016, as part of GCHQ. The Minister for the Cabinet Office subsequently announced in March 2016 that it would be named the “*National Cyber Security Centre*” (NCSC) and that it would open by October that year.

26. In autumn 2016, as part of its routine oversight of GCHQ’s administration and finances, the Committee requested a copy of the business case for the accommodation for the new Centre.[5] Upon reviewing it, it was apparent that the chosen option, Nova South (a new development in Westminster), had a running cost of more than double that of the second choice. The Committee received assistance from the National Audit Office (NAO) in analysing the procurement process, before then questioning GCHQ and the Cabinet Office.

27. The Committee produced the Report, *GCHQ accommodation procurement: a case study*, which was eventually published in November 2020. The Inquiry had discovered very significant shortcomings throughout the procurement process, including an arbitrary timetable, faulty criteria, unjustified score changes, a ‘no-hoper’ alternative and, finally, the Principal Accounting Officer being overruled.

28. The Committee concluded that the selection criteria used were faulty from the outset, with an unnecessarily tight timetable having been imposed arbitrarily, resulting in excessive haste which potentially led to faulty decision-making – and to good options being summarily dismissed due to non-availability within that timescale. Locations outside of London were never considered, and great emphasis was placed on finding high-quality accommodation – without any case being made for why that was necessary. At a late stage, the location requirement was changed to the Westminster area – despite this never being formally

[4] In a speech to GCHQ on 16 November 2015.

[5] The Committee’s remit includes the administration, finances and policy of the seven organisations it oversees. These have usually been reported on in Annual Reports, such as that in 2016–2017, rather than in Special Reports, which have tended to focus on operational matters. However, administration and finances are an important part of the Committee’s remit: if there are problems in these areas then the operational work will suffer. There is no other body that is able to scrutinise these matters, and it is essential that they do receive scrutiny, given the sizeable budget allocated to the Agencies.

specified as a criterion and the case for it not being made. The late switch rendered much of the previous work useless.

29. The Committee was clear that, even disregarding the faulty criteria, GCHQ selected Nova South against all the evidence – and despite warnings that it would neither be ready on time nor had received approval from the Government Property Unit. Nova South was approved at around double the cost of typical government accommodation in London: this was allowed to happen because the scoring system which GCHQ chose significantly underweighted costs and overweighted location. Even then, Nova South did not come out on top in GCHQ's own scoring outcome at the Shortlist stage; at the Draft Full Business Case stage, nine of the ten scores were changed arbitrarily – and in direct contravention of the criteria – in favour of Nova South.

30. Nova South was put into a 'final two' run-off with a complete 'no-hoper'. At the Final Business Case stage, cost-related factors were removed as key criteria and Nova South was therefore put forward despite the fact that it considerably overshot the funds allocated and, critically, will lead to sacrifices in GCHQ's wider spending over the 15-year lease.

31. The Committee also criticised the role of Ministers in the process, the then Chancellor having overruled the then National Security Adviser's strong advice to reject Nova South – he had told the Chancellor that it did not represent value for money, was not deliverable in time and put other national security issues at risk – in order to confirm what GCHQ had made clear was the only option that they would accept.

32. The Report marked a departure from the more operational nature of the Special Reports that have been the focus of the Committee's work in recent years. However, the Agencies receive considerable funding from the Single Intelligence Account (SIA) and they must be careful custodians of public money, just like any other part of government. Procurement processes must be conscientiously conducted and if the Committee has concerns that that might not be the case then it is essential to shine a light on these issues and hold those responsible to account.

Statements

Statement on 5G suppliers

33. In February 2019, the Committee began an Inquiry into the national security issues relating to China. One of the strands of that Inquiry concerned the UK telecommunications network: at the time there was considerable public and parliamentary debate as to whether the Chinese technology company Huawei should be allowed to supply equipment for the UK's 5G network. Given that a government decision was thought to be imminent, the Committee prioritised this aspect of its Inquiry and on 19 July 2019 issued a statement with its findings.

34. The Statement noted that, from amongst our Five Eyes partners, the United States and Australia had already been vocal in their concerns that the UK might employ Huawei within its 5G network. It was emphasised that this is not about any risk to the communication channels which are used for intelligence exchange – these would always be kept entirely separate. It is about perception as much as anything: our Five Eyes partners need to be able to trust the UK and we must not do anything which puts that at risk.

35. The Committee considered that there was a question as to whether other countries might follow the UK's decision, as the UK is a world leader in cyber security: if we were to allow Huawei into our 5G network we must be careful that it is not seen as an endorsement for others to follow.

36. Indeed, one of the lessons the Committee was clear that the UK Government must learn from the debate over 5G is that, with the technology sector now monopolised by such a few key players, the UK is over-reliant on Chinese technology – and the UK is not alone in this; this is a global issue.

37. In the Statement, the Committee urged the Prime Minister to take a decision on which companies will be involved in the 5G network so that all concerned can move forward. In July 2020, a year after the ISC published its Statement, the Secretary of State for Digital, Culture, Media and Sport informed Parliament that the forthcoming Telecommunications (Security) Bill would mean that UK telecommunications operators must stop buying Huawei 5G equipment by the end of 2020, and that Huawei equipment would be removed from the UK's 5G network by 2027:

> *We have previously set out our plans to safely manage the presence of high risk vendors in our 5G network. And of course* [the Government's] *ambition was that no one should need to use a high risk vendor for 5G at all ... Members have sought commitment from the government to remove Huawei equipment from our 5G network altogether ... This is why* [the Government] *have taken the decision that there can be no new Huawei equipment from the end of this year, and set out a clear timetable to exclude Huawei completely by 2027, with an irreversible path implemented by the time of the next election. Telecoms providers will be legally required to implement this by the Telecoms Security Bill, which* [will be brought] *before this House shortly.*[6]

The Bill was introduced on 24 November 2020. At the time of writing, the Bill had reached Committee stage in the House of Lords.

Statement on Detention and Rendition

38. In June 2018, the ISC published two Reports[7] on the actions of the Agencies and Defence Intelligence (DI) in relation to the handling of detainees overseas and rendition. There were over 70 recommendations made between both Reports.

39. In the second of the Reports, which dealt with the situation since 2010, the Committee recommended a full-scale review of the Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees. (The Cabinet Office had conducted a very 'light touch' review of the Guidance in 2017, but the Committee felt that the review was insufficient and the revised draft did not go far enough.) As a result, in June 2018, the Prime

[6] The Secretary of State for Digital, Culture, Media and Sport Oliver Dowden. (14 July 2020). *UK Telecommunications volume 678* [Hansard]. (Volume 678). parliament.uk/House of Commons/2020-07-14/debates

[7] The two Reports published in June 2018 were the *'Detainee Mistreatment and Rendition: 2001–2010'* and *'Detainee Mistreatment and Rendition: Current Issues'*.

Minister had asked the Investigatory Powers Commissioner (Sir Adrian Fulford) to conduct a full review.

40. The Committee was pleased to see that, as a result of their recommendations, and Sir Adrian's review, the Government accepted all the major changes that were required. The Committee noted that the new 'Principles' (published on 18 July 2019) reflect the:

> *important changes we recommended, including for example: specific reference to extraordinary rendition, alongside torture and CIDT;*[8] *the application of the Principles to joint units and non-state actors; regular review; and that the Agencies must follow the spirit of the Principles, not just the letter. This is a major step forward; we are pleased there has been real change as a result of our recommendations.*[9]

Statement on the Covert Human Intelligence Sources (Criminal Conduct) Bill

41. As previously noted, one of the issues considered in the Committee's Report on Northern Ireland-related terrorism – published on 5 October 2020 – was that of agent participation in criminality.

42. At the time of the Inquiry into Northern Ireland-related terrorism, the Investigatory Powers Tribunal (IPT) was considering a case brought by Privacy International and others against the Government, challenging the basis for MI5's ability to authorise agent participation in criminality. On 20 December 2019, the IPT found, with a 3:2 majority, that MI5 does have the implied power – by virtue of the Security Service Act 1989 – to authorise its agents to participate in criminality.[10] While the IPT ruled in favour of the Government, the Government nevertheless decided to introduce legislation to provide a clear and express power to authorise this activity, and on 24 September 2020 introduced the Covert Human Intelligence Sources (Criminal Conduct) Bill.

43. The Committee issued a statement the same day making clear its strong support for the principle behind the legislation, in providing a clear and express power to authorise this activity. However, the Committee was clear that such authorisations must be properly circumscribed, be used only where necessary and proportionate, comply with the Human Rights Act and be subject to proper scrutiny. The Committee's subsequent scrutiny of the legislation is covered below.

Legislation

44. During the period covered by this Report, there have been three pieces of legislation before Parliament in which the Intelligence and Security Committee has an interest:

(i) The Covert Human Intelligence Sources (Criminal Conduct) Act 2021 received Royal Assent on 1 March 2021. This is a vitally important piece of legislation, and – as noted

[8] Cruel, inhuman or degrading treatment.

[9] Statement made by the then ISC Chairman The Rt Hon. Dominic Grieve MP (July 2019). Isc.indepemdnet.gov.uk/news

[10] This decision was later appealed, and in January 2021 the Court of Appeal also found in favour of the Government. The claimants have since indicated their intention to seek an appeal through the Supreme Court.

previously – the Committee fully supports the principle behind it. The Act places on an explicit statutory basis the powers that certain government bodies, such as the police and MI5, already had to authorise criminal activity in carefully controlled circumstances.

Covert Human Intelligence Sources (CHIS) – or agents – provide invaluable information to assist the Agencies and DI in their investigations. They put their lives at risk every day to help keep the country safe. Without them, many of the attacks foiled in recent years would have succeeded in their horrific aims.

While working undercover, CHIS may sometimes need to carry out criminal activity to maintain their cover: they need to be trusted by those they are reporting on so that they can gain the information the authorities need. Their handlers must therefore be able to authorise them to carry out criminal activity in certain circumstances and subject to specific safeguards. The ISC highlighted the importance of these powers in its report on Northern Ireland-related terrorism.

The Committee was satisfied that this Act strengthens the oversight and governance regime for these powers. The Committee scrutinised the legislation, engaging in parliamentary debates at every stage during its passage, and working with the Government to improve the oversight arrangements.

The Government has given a written commitment that the ISC will have oversight of the Criminal Conduct Authorisation policies by the organisations it oversees. The CHIS Code of Practice has also been strengthened in response to concerns raised by the Committee and by parliamentarians in both Houses, and an enhanced oversight role has been provided to the independent Investigatory Powers Commissioner. These are very serious powers for the State to exercise, and it is right that they will be properly scrutinised.

(ii) On 11 November 2020, the National Security and Investment Bill was introduced to the House of Commons.

The Bill sought to establish a new regime for government scrutiny and intervention of investments for the purposes of protecting national security. The Bill sought to give the Secretary of State powers to screen investments if they might pose a national security risk. It was the ISC who first investigated Her Majesty's Government (HMG) powers and processes for scrutinising foreign investment in sensitive areas of UK industry, found them lacking, and called for greater powers.[11] The legislation was therefore a direct result of the Committee's scrutiny and the Committee welcomes the Bill.

However, as introduced, the Bill failed to provide for any scrutiny of these new powers. While the Select Committee for the Department for Business, Energy and Industrial Strategy (BEIS) can oversee the business elements of the Bill, they obviously cannot oversee the security elements of the Bill since they do not have the requisite security apparatus (security-cleared staff, secure storage, accredited meeting space, etc.). Logically, that oversight responsibility can only fall to the ISC, since this Committee was established by Parliament expressly for the purpose of overseeing security matters. The Committee therefore put down an Amendment to the Bill to provide the ISC with oversight of the security elements of the Bill.

[11] This was in the Committee's 2013 Report *'Foreign Involvement in the UK's Critical National Infrastructure'.*

The Government has refused to accept the ISC's oversight role, on the basis that BEIS is not listed in the ISC's remit, and that the BEIS Select Committee is able to provide oversight. Neither of these arguments are correct. While BEIS is not listed in the version of the Memorandum of Understanding (MoU) currently in operation, that is because that MoU was published in 2014 – when neither the Investment Security Unit (ISU) nor BEIS were conducting security-related work. The Government gave a clear undertaking to Parliament during the passage of the Justice and Security Act 2013 (JSA) when the Bill Minister told Parliament that it was "*the intention of the Government that the ISC should have oversight of substantively all of central Government's intelligence and security activities to be realised now and in the future*". The Bill 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*".[12] The Government's commitment to Parliament was that the ISC would oversee all security matters across Government and the MoU would enable that and be kept up to date. The fact that BEIS is not currently listed in the MoU is therefore irrelevant.[13]

The second argument employed was that the BEIS Select Committee is able, and best placed, to provide oversight. However, that Select Committee cannot provide effective oversight given that it cannot regularly or effectively scrutinise Top Secret or intelligence material: whilst a Minister might be able to show the material to Committee Members under the Osmotherly Rules, it would be a security breach for the material to be shown to the Committee Staff (as they do not have the necessary security clearance) or for the Committee to store it themselves or for the Members to discuss it as Committee business (as they do not have the necessary secure premises or arrangements). Without the means to consider the material independently of Government it cannot be considered to constitute oversight, let alone effective oversight. Further, the BEIS Select Committee is not best placed to assess it, since it does not have the context when it comes to security matters.

The third argument raised by the Government was that giving the ISC oversight of this area of work would raise demarcation issues with the BEIS Select Committee. However, this ignores the fact that the ISC already oversees parts of departments which for the most part fall to a departmental Select Committee: Homeland Security Group in the Home Office is just one such example, and the ISC has never had any demarcation issues with the Home Affairs Committee. In this respect, the MoU with the Prime Minister is also entirely clear: "*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 departments such as the Home Office, FCO and MOD by other parliamentary committees*".

The debates on the Bill highlighted that the current MoU, having been published in 2014, is now out of date and requires updating – for example, the Office for Security and Counter-Terrorism mentioned in paragraph 8.b.ii of the MoU is now called Homeland Security Group, and the Intelligence Services Commissioner and the Interception of Communications Commissioner mentioned in paragraph 9 no longer exist. The

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

[13] It is also worth noting that the work which will be carried out by the Investment Security Unit in BEIS is currently being conducted by the Investment Security Group in the Cabinet Office – a team which falls under the ISC's remit.

Committee has therefore raised these issues with the National Security Adviser to address with the Prime Minister, such that the Committee and the Prime Minister can make the necessary updates to the MoU: the changes we have proposed are shown in the draft MoU included at Annex A. These include ensuring that, as intended by the Government and Parliament, the MoU covers those parts of Departments whose work is directly concerned with intelligence and security matters. To ensure that the MoU is not allowed to fall out of date in the future, the Committee will publish the current MoU each year in its Annual Report. This will ensure that the most up-to-date version is easily accessible, and will also provide a regular incentive to ensure that it is kept updated.

The ISC's Amendment to the National Security and Investment Bill was passed by the House of Lords, rejected by the House of Commons and returned to the House of Lords where the Committee chose not to pursue its Amendment, because to do so would have destroyed the Bill. In the interests of national security, we decided not to press our Amendment in the House of Lords because if it had been carried, as it had previously, the Bill would have run out of time and been lost. Nevertheless, we made clear that we will be pursuing the oversight provisions separately: this is a critical issue – if security matters are at the heart of this new legislation, as the Government has said they are, then there needs to be regular and effective oversight of them and only the ISC can provide that oversight. The Bill received Royal Assent on 29 April 2021.

(iii) On 24 November 2020, the Government introduced the Telecommunications (Security) Bill. Again, the legislation directly responds to concerns raised by the Committee (in its 2013 Report on *Foreign Investment in the UK's Critical National Infrastructure*). The Bill establishes a new telecommunications security framework, with new security duties on public telecommunications providers, new powers for the Government to limit or remove vendors from the UK telecoms network, new monitoring responsibilities for Ofcom and strengthened penalties for non-compliance. The same oversight concerns apply as with the National Security and Investment Act, and the Committee will similarly be pursuing these with the National Security Adviser and the Prime Minister. At the time of writing, the Bill had passed Committee stage in the House of Lords.

Areas of inquiry

45. 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-year information covering both the 2018/19 and 2019/20 financial years.

46. We have also been kept updated by the Intelligence Community throughout the year on key developments relating to their work. Given the Committee's focus on its specific Inquiries, detailed scrutiny of each area is not included in this Annual Report; however, the current threat assessment, together with the key facts and major developments for each organisation, are summarised in Annex B and Annex C for 2018/19 and 2019/20 respectively.

China

47. In 2019, the Committee announced that an Inquiry would be held into national security issues relating to China. The Committee received written evidence in April 2019, heard

from leading academic and industry experts in May and June and began questioning the Intelligence Community in July. As noted above, 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.

Extreme Right-Wing terrorism

48. In October 2019, the Committee agreed to undertake an Inquiry considering the threat from what was then termed 'Right-Wing terrorism' (now 'Extreme Right-Wing terrorism'). Written evidence has been received and oral evidence began in December 2020.

International partnerships

49. In October 2019, the Committee agreed to undertake an Inquiry into the role of international partnerships in the work of the UK Intelligence Community. Written evidence was received in November 2020, and the Committee began taking oral evidence in May 2021.

National Audit Office (NAO) evidence

50. As part of the 2015 Spending Review settlement, HM Treasury required the Agencies to deliver £1.3bn in efficiency savings. In response to a request from the Committee, the NAO investigated the Agencies' efficiency savings programme over the course of the Spending Review period and provided the Committee with detailed findings.

51. The NAO found that the Agencies succeeded in meeting the Treasury target of £1.3bn, but that they only did so by including (at the suggestion of the Cabinet Office) *** of foregone investment, which the NAO does not consider to represent a genuine efficiency saving. It appears to the Committee that HM Treasury and the Cabinet Office were not sufficiently realistic in setting the £1.3bn efficiencies target and the extent to which efficiency savings should release cash.[14]

52. The Committee finds it encouraging that the Agencies appear to have made progress in delivering efficiency savings and is encouraged to hear that the effectiveness of the tri-Agency approach to challenging and approving efficiency savings has improved over time. HM Treasury, the Cabinet Office and the Agencies should ensure that clear efficiency savings targets are agreed at the start of future spending periods, with specificity as to what extent such savings should release cash.

Senior staff

53. A number of issues have arisen in recent years surrounding the departure and subsequent behaviour of senior staff within the Intelligence Community which have caused this Committee concern. It is not just the behaviour itself that is of concern, it is the messaging it sends to junior staff about the acceptability of such behaviour, the impact it will have on how the public perceives the Intelligence Community, and the fact that it has not been reported to

[14] The Agencies have since met the target without including the foregone investment.

this Committee as it should have been – as it concerns senior staff it is even more critical that this Committee is informed of it.

54. One such example is the departure of a former Director of GCHQ in 2017. The Committee's concerns were raised when, on 24 February 2019, the *Mail on Sunday* published an article headed "*Theresa May allowed GCHQ spy chief to resign for 'family reasons' after he helped paedophile catholic priest avoid jail – despite media being told he would be 'caring for a sick relative'.*" The newspaper alleged that Mr Hannigan had "*stepped down after the National Crime Agency discovered that he helped a close family friend avoid a custodial sentence for possessing 174 child pornography images ... but Higgins went on to reoffend, and during an NCA probe his links to Mr Hannigan were discovered*". The newspaper subsequently reported – erroneously – on 23 March 2019 that the ISC was investigating the allegations.

55. The previous Committee had indeed asked the Foreign and Commonwealth Office (FCO) in 2017 – when the individual had unexpectedly resigned as Director after such a short tenure – whether there was anything surrounding the resignation of which the Foreign Secretary considered the Committee should be aware. The FCO had assured the Committee that there was nothing further to add beyond the 'family reasons' cited publicly. Following the appearance of the *Mail on Sunday* article in February 2019, the Committee therefore wrote to the NSA to ask why the Committee had been misled on this issue.

56. Initially, the Committee was provided with a short response, which did not answer its question or concerns – namely, whether Mr Hannigan (Director of GCHQ from November 2014) had, whilst at the FCO, given a character reference in his official capacity; the involvement of GCHQ in the investigation of the offender; the involvement of the Director in that investigation; and why the Committee had been misled. Following further inquiries, the NSA informed the Committee that:

- the reference was given in a personal capacity; however, Mr Hannigan had included his FCO title in the reference;
- at the time of his resignation as Director, a further criminal investigation into Father Higgins was in the evidence-gathering phase, before submission to the Crown Prosecution Service for consideration; and
- a limited number of staff in GCHQ, Cabinet Office, Government Legal Department (GLD) and the NCA were aware of the association between the Director and Father Higgins, and "*it would not have been appropriate to share information outside this group, including with the ISC, during the investigation*".

57. While recognising that there was a criminal investigation under way, the Committee considers nevertheless that where the Head of an intelligence Agency steps down unexpectedly, then as the body that is entrusted with oversight of the Intelligence Community, and ensuring their probity, then this Committee must be fully informed of the circumstances. Given the investigative powers with which we trust our Intelligence Community, it is imperative that they are above all suspicion.

58. Of further concern to the Committee are the actions of senior staff when they leave the Agencies and the extent to which they are still bound by their former duties – in particular

when they seek a second career as a 'talking head' on security issues. This first came to the Committee's attention in May 2019, when the former Director of GCHQ appeared in a Channel 4 documentary entitled *The Hunt for Jihadi John*. In that interview he provided operational details as to how the Agencies identified Emwazi. The previous Committee wrote to the Cabinet Secretary asking whether the individual had sought clearance to appear on the programme, and what action was being taken in response to an apparent breach of the Official Secrets Act.

59. The then Cabinet Secretary confirmed that the individual's appearance was "*not endorsed by the Government*". In relation to the provisions of the Official Secrets Act, he noted that the new Director of GCHQ had written to his predecessor to remind him of his ongoing responsibility to safeguard information and to seek approval in advance of discussing matters in the media.[15]

60. It is very surprising to this Committee, knowing how seriously the staff within the Agencies take their duty to safeguard sensitive information, that a previous head of one of those organisations can appear on television and divulge those secrets and yet no substantive action can be taken. It sends entirely the wrong message to those who may be tempted to breach those obligations themselves, and to those who risk their lives to protect them. The question of the obligations of former members of the Intelligence Community – particularly when they seek to build a lucrative career as a commentator on such issues or indeed a lucrative second career in the private sector which utilises the knowledge they have gained – is one which the Committee considers requires further thought and scrutiny since it appears to be possible to breach the current arrangements with no sanctions resulting.

Committee resources

61. The Committee was supported in its work this year by a team of ten staff. The Committee's budget for the 2019/20 financial year was exceptionally – and unauthorised by the Committee – reduced to £1,304,000 by the Cabinet Office (from £1,646,000 in 2018/19). Fortuitously, the Committee's budget covers the costs of the Committee and their staff's security, IT, telecoms, report publication, accommodation, utilities and centrally provided corporate services. Exceptionally, the unauthorised reduction for the 2019/20 financial year did not impact on the work of the Committee due to the lengthy delay in reconstituting the Committee. We have been assured that the full budget has been reinstated now that the Committee has been re-established.

Meeting with the Prime Minister

62. Since its establishment in 1993, the Committee has 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. The Committee regards this as unacceptable given the importance of the issues at hand: we trust the current Prime Minister will recognise this and we have therefore requested a meeting with him this year (2021).

[15] In a letter dated 5 November 2019, from the National Security Adviser (NSA) to the ISC, the NSA confirmed that the Director of GCHQ had written to his predecessor "*following Cabinet Office processes and discussions to ensure proper consideration of potential unauthorised disclosures in light of the applicable law*".

LIST OF WITNESSES

Ministers

The Rt Hon. Priti Patel MP – Secretary of State for the Home Department

The Rt Hon. Dominic Raab MP – then Secretary of State for Foreign, Commonwealth and Development Affairs

Officials

CABINET OFFICE

Sir Simon Gass KCMG CVO – Chair, Joint Intelligence Committee

Ms Madeleine Alessandri CMG – then Deputy National Security Adviser

Dr Christian Turner CMG – then Deputy National Security Adviser

Mr David Quarrey CMG – acting National Security Adviser

Ms Beth Sizeland – Deputy National Security Adviser

Other officials

FOREIGN, COMMONWEALTH AND DEVELOPMENT OFFICE (FCDO)

Sir Philip Barton KCMG OBE – then Director General Consular and Security

Other officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ)

Sir Jeremy Fleming KCMG CB – Director

Mr Ciaran Martin CB – then CEO National Cyber Security Centre

Ms Lindy Cameron – CEO National Cyber Security Centre

Other officials

MINISTRY OF DEFENCE (MoD)

Lieutenant General Sir Jim Hockenhull KBE – Chief of Defence Intelligence

Other officials

SECRET INTELLIGENCE SERVICE (SIS)

Sir Alex Younger KCMG – then Chief

Mr Richard Moore CMG – Chief

Other officials

SECURITY SERVICE (MI5)

Mr Ken McCallum – Director General

Other officials

Expert external witnesses

Nick Lowles MBE – Chief Executive, Hope Not Hate

Jacob Davey, Far Right and Hate Crime Lead, Institute of Strategic Dialogue

The Committee is also grateful to those who provided written evidence, including Professor Matthew Feldman (Director of the Centre for Analysis of the Radical Right), Tom Keatinge (Director of the Centre for Financial Crime and Security Studies at RUSI) and Sara Khan (Commission for Countering Extremism).

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

(SHOWING THE CHANGES 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 Her Majesty's Government (HMG) by the Intelligence and Security Committee of Parliament (ISC).

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

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

The Intelligence and Security Committee of Parliament

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

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

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

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

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

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

Remit

8. The Act provides that the ISC may oversee the expenditure, administration, policy and operations of the Agencies; and that it may examine or otherwise oversee such other activities of HMG in relation to intelligence or security matters as are set out in a Memorandum of Understanding. The ISC is the only committee of Parliament that has regular access to protectively marked information that is sensitive for national security reasons; this means that only the ISC is in a position to scrutinise effectively the work of the Agencies and of those parts of Departments whose work is directly concerned with intelligence and security matters. 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. Ministry of Defence (MoD):

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

(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; co-ordinating 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); and

(ii) the activities of the Joint Intelligence Organisation (JIO).

c. Home Office: the activities of Homeland Security Group (HSG).

d. Department for Business, Energy and Industrial Strategy (BEIS): the activities of the Investment Security Unit.

e. Department for Digital, Culture, Media and Sport (DCMS):

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

(ii) the Office of Communications; and

(iii) the Counter Disinformation Unit.

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

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 co-operate with them so far as is reasonable to avoid any unnecessary duplication in their respective remits.

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

Oversight of operational matters

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

Provision of information

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

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

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

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

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

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 that the ISC needs. The ISC will work together with the Agencies and Departments to ensure that the provision of such information does not involve disproportionate cost or diversion of effort.

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

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

a. Cabinet Office: any Minister of the Crown in a relevant government department;
b. Ministry of Defence: 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. Department for Business, Energy and Industrial Strategy: Secretary of State for Business, Energy and Industrial Strategy;
f. Department of Digital, Culture, Media and Sport: Secretary of State for Digital, Culture, Media and Sport;
g. Department for Transport: Secretary of State for Transport; and
h. Department of Health and 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 inquiries 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 its 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[7], and one that it is expected will be required to be exercised very rarely. In exercising this discretion, the Secretary of State will have particular regard to the provisions that the ISC has for keeping material confidential. In some cases, having regard to those provisions and other features of the ISC that distinguish it from Select Committees, the Minister might well consider it appropriate that information be provided to the ISC. For example, the ISC has in the past received information about matters *sub judice* and/or contained in papers of a previous administration.

Oral evidence sessions: Closed

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

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

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

Open sessions

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

[7] In considering whether to withhold information on these grounds the Secretary of State will have regard to any guidance issued by a Minister of the Crown or a Department concerning the provision of evidence by civil servants to Select Committees (paragraph 4(5) of Schedule 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 Community, HMG will work constructively with the ISC to ensure that as much of its Reports as 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 B: CURRENT 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 international and Northern Ireland-related terrorism, Hostile State Activity, the cyber threat and nuclear proliferation. The Intelligence Community works to counter these threats. The following is a summary of the current threat assessment up to July 2021.[1]

The current threat picture

The UK National Threat Level is currently SUBSTANTIAL, meaning an attack in the UK is likely. Within the reporting period, the UK National Threat Level was raised on 3 November 2020 to SEVERE: an attack is highly likely, reflecting the risk of attacks in France and Austria having a galvanising effect on UK-based extremists. The National Threat Level was then lowered on 8 February 2021. The UK continues to face a high level of terrorist threat which is increasingly diverse in its ideological influences, potential attack methodologies, and targets chosen by extremists. There were four Islamist terrorist attacks during this period: the attack at Fishmongers' Hall, London in November 2019, in which two individuals were killed by Usman Khan; a non-fatal attack in HMP Whitemoor in January 2020; an attack in Streatham, London in February 2020, where the attacker Sudesh Amman was killed; and an attack in Reading in June 2020, when three individuals were killed by Khairi Jamal Mohamed Saad-Allah (the extent to which Saad-Allah's attack was driven by ideology, rather than his own mental health situation, remains not wholly clear). There was also one failed Extreme Right-Wing terrorist attack on a solicitor's office in September 2020. The primary terrorist threat to the UK continues to be from Islamist terrorism. ISIL-Core (Daesh) has continued to operate as a clandestine terrorist organisation despite the death of its leader Abu Bakr al-Baghdadi in October 2019. ISIL aspires to re-establish its Caliphate and to sustain a global network of supporters that enables it to promote a narrative of enduring success. ISIL continues to aspire to mount attacks against Western countries including the UK. ISIL media proliferates online and its ideology continues to inspire low-sophistication actors in the UK and within Europe to conduct attacks. Al-Qaeda (AQ) continues to embed itself in local conflicts, particularly in Africa, providing a platform for further terrorist activity by the group. AQ's network of global affiliates represents a significant threat to UK nationals and interests overseas. AQ's ultimate aim remains to establish a global Caliphate. The threat from ISIL and AQ as global franchises is likely to endure, with both groups increasingly trying to leverage regional networks to advance their strategies. They will continue to present multi-faceted threats and to be active in multiple theatres, which will project a threat to the UK, and to UK interests, in diverse ways. Separately, there is an enduring threat from Extreme Right-Wing terrorism and, to a lesser extent, Left-Wing, Anarchist and Single Issue terrorism (LASIT). The Home Secretary has proscribed a small number of Extreme Right-Wing terrorist groups that have an overtly violent ideology. Following the proscription of National Action

[1] The Joint Terrorism Analysis Centre (JTAC) assesses the threat from all forms of terrorism. There is a single National Threat Level describing the threat to the UK, which includes Islamist, Northern Ireland, Left-Wing and Extreme Right-Wing terrorism. MI5 is responsible for setting the threat levels from Irish and other domestic terrorism both in Northern Ireland and in Great Britain. 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).

in 2016, two other groups, Sonnenkrieg Division (SKD) and Feuerkrieg Division (FKD), were proscribed in 2020. These groups promote their ideology online through violent propaganda, commonly targeting young people. The groups often use mainstream social media platforms to post non-extreme material with the intention of engaging younger audiences before encouraging them to move to less moderated platforms where more graphic and extreme content is shared. It continues to be most likely that an Islamist or Extreme Right-Wing terrorist attack would emanate from self-initiated terrorists who plan and conduct attacks independently of any formal association with a wider terrorist group.

Northern Ireland-related terrorism

The threat level in Northern Ireland (NI) from Dissident Republican (DR) groups remains unchanged at SEVERE, meaning an attack is highly likely. This has remained at the same level since 2009 and requires constant security force pressure to keep it suppressed. The trajectory of the threat is now broadly stable after several years of gradual decline. 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: New IRA and Continuity IRA (CIRA) continue to drive the threat picture. Whilst other DR groups still exist, such as Arm na Poblachta (ANP) and Oglaigh na h'Eireman (ONH), the threat they pose to national security has reduced. As well as their direct threat to national security, all of these groups are involved in the same types of harmful serious criminal activity, violence and intimidation as those currently on ceasefire. 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 clear and rising risk that discontent in the Loyalist community, which has already given rise to episodes of violent disorder, could escalate further and translate into a renewed national security threat.

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 recently passed National Security and Investment Act gives 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 by developing a Counter State Threats Bill.

The cyber threat

Cyber is a vector used both by hostile state actors and criminals to steal information, data and intellectual property, and as such is an increasing and significant threat to the UK. The COVID-19 pandemic fast-tracked a societal shift already under way towards greater reliance on online services for working, shopping and socialising. This has meant a whole range of companies and business areas shifting policies about what they can do online. Whilst the media has highlighted the relative ease with which supposedly secure online meetings could be hijacked, the more serious risk comes from hostile state actors who have identified these shifts as an opportunity for cyber attacks. The advent of the COVID-19 pandemic has seen attempts by foreign states to undermine public faith in COVID-19 vaccines. The global dependence on vaccine development has also led to an increased risk in Hostile State cyber activity against the pharmaceutical industry, especially relating to vaccine development and associated supply chains. In September, the United States charged Chinese and Malaysian nationals for engaging in such activity, leading to arrests. A particular focus for the UK Intelligence Community has been on protecting the medical and pharmaceutical sectors from espionage against their work to counter COVID-19. Malware, including ransomware, has become more readily available offering opportunities for less sophisticated operators such as criminal gangs. This year, the National Cyber Security Centre (NCSC) reported a threefold increase in ransomware incidents with government, companies and individuals being targeted in a more aggressive manner than previously seen. Recognising the cyber-enabled threat, in November the UK announced the formation of the National Cyber Force (NCF) to conduct cyber operations to disrupt Hostile State Activity, terrorism and criminality that threatens national security. The NCF combines UK cyber expertise from GCHQ, the MoD, SIS and the Defence Science and Technology Laboratory (DSTL) under a unified command. The cyber-enabled threat will continue to be an important vector for hostile state actors and criminals: during the reporting period, a supply chain attack on SolarWinds, an IT management company, allowed attackers persistent access to hundreds of servers globally, including public sector organisations, over a period of several months. Organisations will continue to embrace working from home with associated cyber risks; we expect states and criminals to seek advantage from this situation. Government, business and academia will need to continue to work together to develop the systems and embed the policies to protect their most valuable information.

Proliferation of weapons of mass destruction

Countering the proliferation of weapons of mass destruction (WMD) continues to be a cross-government priority. The UK Intelligence Community and government departments work both domestically and internationally to prevent the acquisition and supply of equipment and material of potential use to WMD programmes.

ANNEX C: EXPENDITURE, ADMINISTRATION AND POLICY – 2018/19 AND 2019/20

<table>
<tr><th colspan="2">Single Intelligence Account</th></tr>
<tr><th colspan="2"><em>Expenditure in 2018/19</em></th></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>2,563,525</td><td>606,682</td><td>3,170,207</td></tr>
<tr><td>Outturn</td><td>2,550,252</td><td>602,208</td><td>3,152,460</td></tr>
</table>
</td></tr>
<tr><td>Expenditure by category</td><td>● Administration spending: £75m
● Staff pay: £1bn
● Capital spending: £602m</td></tr>
</table>

<table>
<tr><th colspan="2">Single Intelligence Account</th></tr>
<tr><th colspan="2"><em>Expenditure in 2019/20</em>[1]</th></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>2,843,285</td><td>644,100</td><td>3,444,232</td></tr>
<tr><td>Outturn</td><td>2,755,490</td><td>636,423</td><td>3,391,913</td></tr>
</table>
</td></tr>
<tr><td>Expenditure by category</td><td>● Administration spending: £77.5m
● Staff pay: £1.09bn
● Capital spending: £636m</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.

[1] This year, the Committee is reporting on financial information for both 2018/19 and 2019/20, due to the extended period covered by this Report.

MI5 (Security Service)

Expenditure in 2018/19[2]

Total budget and outturn

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

Expenditure by category

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

Expenditure in 2019/20[3]

Total budget and outturn

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

Expenditure by category

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

Administration

Staff numbers[4]

	Total staff[5]	SCS[6]	Non-SCS
31 March 2018	4,416	50	4,366
31 March 2019	4,611	56	4,555
31 March 2020	5,200	76	5,124

Recruitment in 2018/19

- MI5 recruited 504 staff against a target of 450 in 2018/19.
- This compares with 459 staff recruited in 2017/18 against a target of 550.

Recruitment in 2019/20

- MI5 recruited 458 staff against a target of 345 in 2019/20.

Major projects in 2018/19

- To improve the exploitation and retrieval of MI5's information (in progress).
- A programme to deliver the changes required for MI5 to continue to operate compliantly and effectively under the Investigatory Powers Act 2016. The programme has been set up to deliver a coherent and complementary cross-Agency implementation solution.

[2] As reported to the Committee in MI5's end-year report for the 2018/19 financial year.

[3] As reported to the Committee in MI5's end-year report for the 2019/20 financial year.

[4] 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 2019/20 of ***.

[5] There is a significant increase in the total number of staff in 2020, as some GCHQ and SIS staff have transferred across into a shared team hosted by MI5, ***.

[6] Senior Civil Service.

Major projects in 2019/20	● A project to establish a new Counter-Terrorism Operations Centre that will bring together all counter-terrorism (CT) partners (law enforcement and intelligence agencies) to deliver a change in how they work together, with an agile and integrated operational CT response. ● *** ● A programme for the Agencies to deliver key agreed objectives for Spending Review 2015. It delivers "*excellent and efficient corporate services*" at a scale to meet the demands of the UK Intelligence Community. The programme is making good progress with risks and challenges being addressed. In March 2020, with the onset of COVID-19, delivery was temporarily delayed ***.
Diversity and inclusion 2018/19	● Within the recruitment process, a wide range of diversity initiatives are deployed to increase applications from under-represented groups. A marketing strategy has been developed to increase usage of diversity-focused media channels. ● MI5 engaged with external Diversity and Inclusion experts to review (through a BAME lens) their promotion process for middle and senior managers. MI5 has embedded recommended best practices within the hiring process and has taken steps to increase the diversity of hiring panel 'independents' with more BAME employees of mixed grades joining this cadre. ● MI5's diversity progress continues to be externally recognised and has achieved a number of awards such as: Employer of the Year Award at British LGBT awards, Stonewall Top 100 Employers (4th Place), The Times Top Employers for Women and Best Employers for Race.
Diversity and inclusion 2019/20	● In February 2020, MI5 published its second Gender Pay Gap Report along with its first Ethnicity Pay Gap Report. ● MI5 exceeded its recruitment targets and continued to improve female and BAME representation within the organisation. ● Launched MI5's first Diversity Internship for applicants from BAME and lower socio-economic backgrounds. ● MI5 successfully launched its new social mobility network in 2020.
Policy	
Allocation of effort at 31 March 2019[7]	Allocation of effort across three operational themes: ● Islamist terrorism – 70% ● Northern Ireland-related terrorism – 19% ● Hostile State Activity – 11%
Allocation of effort at 31 March 2020[8]	Allocation of effort across three operational themes: ● Islamist terrorism – 68% ● Northern Ireland-related terrorism – 19% ● Hostile State Activity – 13%

[7] Operational allocation of effort (by spend, to the nearest per cent).
[8] Operational allocation of effort (by spend, to the nearest per cent).

<table>
<tr><td>Major achievements reported to the Committee for 2019/20[9]</td><td>● In addition to the live intervention on the Streatham attack, MI5 and police partners have proactively disrupted a further Islamist terrorist plot since January 2020. This brings the total number of Islamist terrorist plots disrupted to 18 since the Westminster Bridge attack in March 2017.
● From January 2020 to June 2020 there have been six successful prosecutions brought against subjects of interest.
● MI5 has worked closely with Intelligence Community partners and other HMG departments during the transition phase of the UK's withdrawal from the European Union (EU), engaging specifically on Agency-related capability concerns, such as data access and the retention of specific EU tools and measures.</td></tr>
<tr><td colspan="2"><b><i>COVID-19 impact</i></b></td></tr>
<tr><td colspan="2">Despite a slowdown due to COVID-19 (within recruitment pipelines), as a result of not being able to conduct face-to-face interviews, the pandemic has presented MI5 with opportunities to modernise and improve its ways of working with joint recruitment functions.
Many training programmes and processes have been adapted quickly to allow delivery remotely.
Implementations of the Compliance Improvement Programme recommendations (set out in Sir Martin Donnelly's Independent Compliance Improvement Review) have been delayed in agreement with the Home Office.
Immediately prior to lockdown, MI5 rapidly rolled out access to the new *** that was developed prior to the COVID-19 crisis. The environment runs at ***.
***.</td></tr>
</table>

[9] Major achievements for 2018/19 were published in the Committee's Annual Report 2018–19.

Secret Intelligence Service (SIS)

Expenditure in 2018/19[10]

Total budget and outturn

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

Expenditure by category

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

Expenditure in 2019/20[11]

Total budget and outturn

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

Expenditure by category

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

Administration

Staff numbers[12]

	Total staff	SCS	Non-SCS
31 March 2018	2,866	83	2,783
31 March 2019	3,063	74	2,989
31 March 2020	4,107[13]	85	4,022

Recruitment in 2018/19

- SIS recruited *** new full-time equivalent (FTE) staff against a target of *** in 2018/19.
- This compares with the recruitment of *** new staff against a target of *** in 2017/18.

Recruitment in 2019/20

- SIS recruited *** new FTE staff against a target of *** in 2019/20.

Major projects in 2018/19 and 2019/20[14]

- A project to deliver a contract to service the needs of the Agencies for contingent labour resource (CLR) was completed in April 2020.
- Data analytics will enable mission teams to improve their performance across the operational cycle, irrespective of whether they work single-service, cross-Agency or with wider partners in policing, defence and overseas.
- A programme of work to rationalise and increase the capacity of the London estate, to enable flexible ways of working, to promote closer working with Whitehall departments, and to co-locate some Agency capabilities as part of the wider strategy.

[10] As reported to the Committee in SIS's end-year report for the 2018/19 financial year.

[11] As reported to the Committee in SIS's end-year report for the 2019/20 financial year.

[12] These figures refer to the number of full-time equivalent (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 2019/20 of ***.

[13] This figure includes ***.

[14] Information taken from SIS 2018/19 and 2019/20 Snapshot Reports.

Diversity and inclusion 2018/19	● Chief of SIS explicitly promoted diversity in public messaging. ● Increased the number of Inspiring Women Leaders and BAME Inspiring Leader Programmes. ● Achieved a number of benchmarking accolades: Stonewall, Business in the Community Race and Gender; and signed up to MIND's 'Time to Change' pledge. ● Through careful negotiation and management, SIS increased diversity in its global network.
Diversity and inclusion 2019/20	● SIS achieved a number of benchmarking accolades such as: Stonewall – recognised as a Top 100 Inclusive Employer, Social Mobility Index placed 73rd. ● SIS published its Gender Pay Gap report on the SIS website. ● There has been an introduction of BAME-focused fast tracking through the recruitment and vetting process. ● SIS published an internal report called Everyday Sexism. ● Training workshops were held for Inclusion and Diversity representatives and contact officers.
Policy	
Allocation of effort at 31 March 2019	● Key operational activities including: counter-terrorism; cyber and access generation; defence technology and counter-proliferation; and prosperity and economic stability – 33% ● Operational support including: global network enabling; covert operations; data exploitation; operational security; and operational technology – 26% ● 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 – 41%
Allocation of effort at 31 March 2020	● Key operational activities including: counter-terrorism; cyber and access generation; defence technology and counter-proliferation; and prosperity and economic stability – 33% ● 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 – 39%
Major achievements reported to the Committee for 2019/20[15]	● Collaboration with partner agencies to provide insight on joint operations. ● Developing technology being used successfully by UK law enforcement in their efforts to tackle terrorist and serious organised crime activity. ● Computer Network Exploitation (CNE) capability continues to contribute to operations during COVID-19. ● Collaboration with HMG to facilitate an international coalition in support of *** against hostile activity.

[15] Major achievements for 2018/19 were published in the Committee's Annual Report 2018–2019.

COVID-19 Impact

The vast majority of the workforce was ***. Immediate priority was to create a ***.

The disruption of the COVID-19 lockdown period presented "*challenges and opportunities*"[16] implementing change that supports SIS strategy and long-term goals (innovation in espionage). Governance and management were adapted through this period to ensure that SIS could react quickly to changing front-line requirements and wider challenges related to COVID-19.

[16] Information taken from SIS 2018/19 and 2019/20 Snapshot Reports.

Government Communications Headquarters (GCHQ)

Expenditure in 2018/19[17]

Total budget and outturn

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

Expenditure by category[18]

- Programme costs (including staff costs, military manpower, purchase of goods and services, and non-cash and other programme costs): ***
- Administration costs: ***
- Capital costs: ***
- Total spend on contracts with external companies: ***

Expenditure in 2019/20[19]

Total budget and outturn

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

Expenditure by category

- Programme costs (including staff costs, military manpower, purchase of goods and services, and non-cash and other programme costs): ***
- Administration costs: ***
- Capital costs: ***
- Total spend on contracts with external companies: ***

Administration

Staff numbers[20]

	Total staff	SCS	Non-SCS
31 March 2018	6,348	82	6,266
31 March 2019	6,791	91	6,700
31 March 2020	7,107	94	7,013

Recruitment in 2018/19

- GCHQ recruited 798 staff against a target of 792 in 2018/19.
- This compares with recruiting 686 new staff against a target of 612 in 2017/18.

Recruitment in 2019/20

- GCHQ recruited 531 staff against a target of 527 in 2019/20.

[17] As reported to the Committee in GCHQ's end-year report for the 2018/19 financial year.

[18] While the Committee's Annual Report 2017–2018 included Annually Managed Expenditure (AME) as a category of expenditure for GCHQ, this has not been included here as AME is not included in the resource and capital spending figures provided in the table above.

[19] As reported to the Committee in GCHQ's end-year report for the 2019/20 financial year.

[20] These figures refer to the number of FTE staff as at the end of the financial year. GCHQ also employs a substantial number of contractors who are not included in these figures.

Major projects in 2018/19[21]	● The CNE scaling programme, to move GCHQ towards a focus on operations that are conducted on the internet using computer network exploitation techniques. ● The High-End Data Centre Capability, involving the creation of a new high-end data centre (in progress). ● A cross-community initiative led by GCHQ to bring together, where appropriate, the provision of technology and services across the three Agencies, enabling enhanced operational performance and delivering efficiencies.
Major projects in 2019/20[22]	● A project that provides secure accommodation for GCHQ staff in Heron House in Manchester city centre. This project is part of the wider 2016 Accommodation Strategy to develop a significant presence of *** staff in the North West over the next five to ten years. ● The CNE scaling programme (part of the GCHQ strategy to become a more active organisation, conducting operations on the internet). Tranche 2 has now commenced, aiming to upscale capabilities for much greater mission impact. ● A cross-community IT initiative is progressing against a complex and changing backdrop of demands, expansion and new location requirements and has reached key milestones for 2019/20 to enable the Agencies to achieve its Spending Review 2015 efficiency targets through infrastructure changes.
Diversity and inclusion 2018/19	● Launch of REACH – a new staff affinity network for BAME colleagues. ● ATTRACT – a women's recruitment campaign aimed at attracting more women to join GCHQ. There was an *Evening Standard* podcast to promote senior women in technical roles. ● Launch of cohort 3 of the CATALYST programme for aspiring female technical leaders. The programme is to develop home-grown technical talent to increase the number of women in senior roles.
Diversity and inclusion 2019/20	● Against its three strategic objectives for 2019 (attract, retain and progress more women, particularly in our technical roles; improve recruitment and progression of ethnic minority staff; and create a more inclusive GCHQ, where everybody is able to see their future), GCHQ has made notable progress against its recruitment and progression priorities, with the recruitment team improving its ability to directly connect with candidates through the recruitment pipeline. ● GCHQ REACH network has worked hand-in-hand with the recruitment team to include an ethnic minority (EM) member of staff at each interview panel for EM candidates. This has made the interview process more inclusive. ● REACH network hosted the Agencies' first BAME conference in May 2019. ● Developed an Inclusive Practice Programme aimed at all staff and designed to accommodate various working locations and patterns. ● Director GCHQ has become GCHQ's first Inclusion Champion.

[21] Information taken from GCHQ 2018/19 Snapshot Report.
[22] Information taken from GCHQ 2019/20 Snapshot Report.

Policy	
Allocation of effort at 31 March 2019	● Mission-specific programmes including: counter-terrorism; Offensive Cyber; serious organised crime; and counter-proliferation – *** ● Capability exploitation[23] – 19% ● Engineering – 18% ● IT services – 7% ● Cyber security – *** ● Corporate services (including human resources and finance) – 20%
Allocation of effort at 31 March 2020	● Mission-specific programmes including: counter-terrorism; Offensive Cyber; serious organised crime; and counter-proliferation – *** ● Capability exploitation – 20% ● Engineering – 18% ● IT services – 7% ● Cyber security – *** ● Corporate services (including human resources and finance) – 19%
Major achievements reported to the Committee for 2019/20[24]	● GCHQ celebrated its Centenary with a number of events, from the opening of the London Science Museum exhibition 'Top Secret: From Ciphers to Cyber Security' to a visit from His Royal Highness the Prince of Wales to GCHQ Benhall. ● As part of the 75th Anniversary of VE Day, GCHQ revealed the last recoded message intercepted from a German military communications network in the Second World War, the Brown Network. ● As part of the transition from the National Offensive Cyber Programme (NOCP) to the National Cyber Force (NCF), GCHQ has formally closed the NOCP. This will be a distinct operational entity, a partnership between GCHQ and the MoD incorporating elements from SIS and the Defence Science Technology Laboratory (DSTL). ● The National Cyber Security Centre (NCSC) was able to adapt quickly to lockdown conditions and shift focus to support the national COVID-19 response supporting individuals and organisations on how to deal with related malicious cyber activity. Many services are being used to help protect UK essential services, from the NHS to universities (which were researching vaccines) and supermarket logistics companies.
COVID-19 impact	
COVID-19 has caused GCHQ to undertake a significant re-orientation of peacetime business. GCHQ quickly adjusted its posture and re-prioritised efforts to safeguard its most critical capabilities, underwritten by feasible and proportionate levels of compliance assurance. This approach reflects the significantly reduced size of GCHQ's workforce conducting operational work and the pressure on those limited numbers to maintain its highest priority missions. The Investigatory Powers Commissioner's Office has been made aware of arrangements and they have been made available for routine independent inspection.[25]	

[23] Capability exploitation is the process of finding and exploiting both secret and open source information in support of intelligence and security missions and ensuring that GCHQ remains at the cutting edge of tradecraft and technology.

[24] Major achievements for 2018/19 were published in the Committee's Annual Report 2018–2019.

[25] Taken from GCHQ consolidated Quarterly Reports to the ISC (January–June 2020).

Defence Intelligence (DI)[26]

Expenditure in 2018/19

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	346,494	1,593	348,087
Outturn	350,494	833	351,327

Expenditure by category

- Operational staff costs: £227.8m
- Other operational costs: £35.4m[27]
- Research and development: £55.9m
- Administration: £36.3m
- Against this, DI received income of £24.8m

Expenditure in 2019/20

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	354,794	498	355,292
Outturn	363,111	177	363,288

Expenditure by category

- Operational staff costs: £249.2m
- Other operational costs: £59.6m
- Research and development: £31.7m
- Administration: £30.3m
- Against this, DI received income of £25.6m

Administration

Staff numbers[28]

				Armed Forces		Civilian staff	
	Total staff	Total civilian staff	Total Armed Forces staff	SCS equivalent	Non-SCS equivalent	SCS	Non-SCS
31 March 2018	3,905	1,299	2,606	6	2,600	7	1,292
31 March 2019	3,904	1,424	2,480	9	2,471	6	1,418
31 March 2020	4,089	1,436	2,653	9	2,644	9	1,427

Recruitment in 2018/19

- In 2018/19, 232 civilian personnel were recruited – the same number as were recruited in 2017/18.

Recruitment in 2019/20

- In 2019/2020, DI reported that 198 civilian personnel were recruited.[29]

Major projects 2018/19

- Programme to rationalise and integrate the DI estate 2 (PRIDE2).

Major projects 2019/20

- Programme to rationalise and integrate the DI estate 2 (PRIDE2).

[26] Information has been reported to the Committee from Defence Intelligence's end-year report for the 2018/19 and 2019/20 financial years.

[27] Other operational costs include equipment support both for 2018/19 and 2019/20 expenditure.

[28] These figures refer to the number of FTE staff as at the end of the financial year. DI also employed a number of contractors and/or consultants. These figures are not included but have estimated costs for 2019/20 of £7m.

[29] Military manning is conducted centrally and the DI military staff is subject to the posting policy of the three Armed Forces. DI does not recruit military staff.

Diversity and inclusion 2018/19	● A Wellbeing, Diversity and Inclusion team was established.
Diversity and inclusion 2019/20	● The Wellbeing, Diversity and Inclusion team increased in size to form part of the DI People team. ● Work has been completed to mandate that all civilian interview panels have BAME representation. ● The number of Mental Health First Aiders increased and a mindfulness programme was also developed. ● DI has increased the number of female and BAME Senior Civil Servants.
Policy	
Allocation of effort at 31 March 2019	● Total operational and analysis effort – 83%. This comprises: − All source analysis and assessment – 10% − Collection and analysis – 73% ● Operational support – 12%. This comprises: − Armed Forces security and intelligence training – 10% − Armed Forces intelligence policy and future capability development – 2% ● Central support – 5%
Allocation of effort at 31 March 2020	● Allocation of effort was the same for 31 March 2020 as it was for 31 March 2019.
Major achievements reported to the Committee for 2019/20[30]	● NCF launched at the start of the financial year. A new operational partnership between GCHQ, the MoD, elements of SIS and the DSTL. ● Russia – Supported UK policy-makers as they shaped NATO policy in response to Russian missile developments and the prospective breakdown of the international strategic arms control framework. ● Counter-intelligence – Continued to build an understanding of the espionage threats to the UK resulting from Russia's participation on conventional arms control treaties including assessment of the intelligence advantage gained by Russia through the Open Skies Treaty. The work has supported both HMG's Russia policy unit and the Joint MoD Counter-intelligence/MI5 response. ● Provided a range of intelligence support to HMG and Allied partners covering issues such as Chinese global influence activities, the conflicts in Syria and Libya, the security of merchant vessels in the Straits of Hormuz, and the aftermath of the death of Major General Qasem Soleimani. ● Provided a significant breadth of intelligence support to the UK Armed Forces' deployment to the United Nations Mission in Mali.

[30] Major achievements for 2018/19 were published in the Committee's Annual Report 2018–2019.

COVID-19 impact

- Output reduced across DI’s portfolio due to reduced staff presence in office (10% at the lowest point). However, key parts of DI sustained output, often compensating for reductions elsewhere in Whitehall.
- DI has supported HMG’s response to COVID-19. Established a separate, central COVID-19 assessment team.
- Provided technical expertise to most UK COVID-19 intelligence activities.
- DI product has provided critical insight directly to the UK Vaccines and Therapeutics Taskforce.

<table>
<tr><th colspan="2">National Security Secretariat (NSS)</th></tr>
<tr><th colspan="2"><em>Expenditure in 2018/19</em>[31]</th></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>9,855</td><td>0</td><td>9,855</td></tr><tr><td>Outturn</td><td>10,620</td><td>0</td><td>10,620</td></tr></table></td></tr>
<tr><td>Expenditure by category</td><td>● Pay costs: £7.6m
● National Cyber Security Programme: £2.6m</td></tr>
<tr><th colspan="2"><em>Expenditure in 2019/20</em>[32]</th></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>12,879</td><td>0</td><td>12,879</td></tr><tr><td>Outturn</td><td>12,451</td><td>0</td><td>12,451</td></tr></table></td></tr>
<tr><td>Expenditure by category</td><td>● Pay costs: £10.8m
● National Cyber Security Programme (NCSP): £3.8m</td></tr>
<tr><th colspan="2"><em>Administration</em></th></tr>
<tr><td>Staff numbers[33]</td><td><table><tr><th></th><th>Total staff[34]</th><th>SCS</th><th>Non-SCS</th></tr><tr><td>31 March 2018</td><td>121</td><td>17</td><td>104</td></tr><tr><td>31 March 2019</td><td>146</td><td>24</td><td>122</td></tr><tr><td>31 March 2020</td><td>190</td><td>26[35]</td><td>164</td></tr></table></td></tr>
<tr><td>Recruitment in 2018/19</td><td>● NSS recruited 74 staff in 2018/19.
● This compares with 31 staff recruited in 2017/18.</td></tr>
<tr><td>Recruitment in 2019/20</td><td>● NSS recruited 49 staff in 2019/20.</td></tr>
<tr><td>Major projects in 2018/19</td><td>● None reported.</td></tr>
<tr><td>Major projects in 2019/20</td><td>● None reported.</td></tr>
<tr><td>Diversity and inclusion 2018/19</td><td>● The NSS appointed a Diversity and Inclusion lead.</td></tr>
<tr><td>Diversity and inclusion 2019/20</td><td>● NSS is part of the National Security Culture Enquiry and is linked to a number of initiatives in Cabinet Office such as reverse BAME mentors for SCS and both Deputy National Security Advisers (DNSAs) are champions across Cabinet Office for the LGBTQ+ Network and Wellbeing Network.</td></tr>
</table>

[31] As reported to the Committee in NSS’s end-year report for the 2018/19 financial year.

[32] As reported to the Committee in NSS’s end-year report for the 2019/20 financial year.

[33] These figures refer to the number of 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 2019/20 of £330,000.

[34] 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.

[35] Includes one SCS 4 – National Security Adviser.

Policy	
Allocation of effort at 31 March 2019	● Operational (policy teams and private offices) – 81% ● Corporate services – 19%
Allocation of effort at 31 March 2020	● Operational (policy teams and private offices) – 83.7% ● Corporate services – 16.3%
Major achievements reported to the Committee for 2019/20[36]	● A DNSA led a team of National Security Directors in a bilateral security dialogue with the French. ● Significant developments towards the signing of the UK–US Bilateral Data Access Agreement – a key national security priority – including the Royal Assent of the Crime (Overseas Production Orders) Act in February 2019.[37] The UK–US Bilateral Data Access Agreement passed the scrutiny periods in both the UK Parliament and the US Congress with no opposition. ● Much of COVID-19 has shaped the Government's cyber security work in this period, with malicious actors exploiting the pandemic by targeting individuals and organisations with a range of scams, ransomware and malware. Therefore, through the National Cyber Security and Strategy Programme across government, they have: worked closely with the NHS to keep its systems and the healthcare sector safe; published technical guidance; identified and removed malicious sites associated with COVID-19 threats; and worked with partners to counter Hostile State Activity in the UK and abroad.

COVID-19 impact

At the outset of the crisis response to the COVID-19 pandemic, members of many Cabinet Secretariat teams were temporarily redeployed to support COVID-19 structures. The impact on staffing numbers varied significantly between teams and over time. Within the National Security Unit (NSU), 50% of the 88 staff were redeployed in the immediate response. The unit retained a core set of staff, organised to ensure flexibility to respond to shifting priorities, and resources in the event of a serious national security incident. New ways of working were put in place to adhere to social distancing requirements, but teams have continued to deliver essential responsibilities.

COVID-19 resulted in the Agencies delaying the production of their annual resource accounts which had been completed with the Cabinet Secretary, HM Treasury and National Audit Office (NAO) approval. Draft outturn figures were produced in July 2020 ahead of the delayed NAO audit scheduled in August/September 2020.

The Integrated Review was announced in February 2020, but was paused in April 2020 due to the need to focus on COVID-19. The review formally recommenced in June 2020 (and was published in March 2021).

***.

[36] Major achievements for 2018/19 were published in the Committee's Annual Report 2018–2019.

[37] The UK–US Bilateral Data Access Agreement was subsequently signed on 3 October 2019.

From March 2020, some NSS international engagement work was paused to allow teams and key partners to focus on the response to COVID-19; other engagement work went ahead virtually. This included work across Europe and with Five Eyes partners. In June, Five Eyes work picked up ***.

COVID-19 shaped much of the Government's cyber community's work in the reporting period and necessitated refocused efforts (and investments) within the team into particular areas.[38]

[38] Taken from NSS Quarterly Reports to the ISC (January–June 2020).

Joint Intelligence Organisation (JIO)

Expenditure in 2018/19[39]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	6,007	0	6,007
Outturn	6,100	(3)	6,097

Expenditure by category

- Pay costs: £4.9m
- Travel: £0.236m
- The remaining outturn is accounted for primarily through accommodation/estates, refurbishment, staff training and other administrative costs.

Expenditure in 2018/19[40]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	9,261	20	9,281
Outturn	9,088	(10)	9,078

Expenditure by category

- Pay costs: £7m[41]
- Travel: £0.246m
- The remaining outturn is accounted for primarily through accommodation/estates, staff training and other administrative costs.

Administration

Staff numbers[42]

	Total staff	SCS	Non-SCS
31 March 2018	79	8	71
31 March 2019	91	9	82
31 March 2020	111	11	100

Recruitment in 2018/19	● The JIO recruited 32 new staff in 2018/19 (an increase in its overall headcount of 26 FTE staff). ***. ● This compares with 19 staff recruited in 2017/18, ***.
Recruitment in 2019/20	● The JIO recruited 43 new staff in 2019/20. ***.
Major projects in 2018/19	● None reported.
Major projects in 2019/20	● None reported.
Diversity and inclusion achievement 2018/19	● Launched a dedicated Diversity and Inclusion Network working across JIO teams and the national security community.

[39] As reported to the Committee in the JIO's end-year report for the 2018/19 financial year.

[40] As reported to the Committee in the JIO's end-year report for the 2019/20 financial year.

[41] The increase in pay costs this year is the result of the 2019 uplift of 26 posts and a more aggressive approach to recruitment which has resulted in fewer posts being gapped and longer handovers.

[42] These figures refer to the number of FTE staff as at the end of the financial year. JIO also employed a number of contractors and/or consultants. These figures are not included but have estimated costs for 2019/20 of £80,000.

Diversity and inclusion achievements 2019/20	● The Joint Intelligence Committee (JIC) considered a JIO assessment on how to improve Diversity and Inclusion in the national security community and the paper has been used as the key evidence base for the National Security Council Diversity and Inclusion Steering Group's action plan.
Policy	
Allocation of effort at 31 March 2019[43]	● Total operational activity – 94% ● Corporate services (including central support and intelligence profession) – 6%
Allocation of effort at 31 March 2020	● Total operational activity – 94.5% ● Corporate services (including central support and intelligence profession) – 5.5%
Major achievements reported to the Committee for 2019/20[44]	● JIO continued to provide all-source assessment to inform policy decisions on national security. This included assessment both of specific events and strategic outlook. To achieve this, JIO developed new formats and approaches to meet customer needs. ● In November and December 2019, JIO convened the domestic and international assessment communities to develop a strategic outlook to 2030 across a wide range of national security areas. ● JIO produced its first JIC paper examining Diversity and Inclusion in the national security community in January 2020. ● JIO hosted an annual conference for Five Eyes assessment partners in June 2019, as well as a conference focused on emerging technology in December 2019. ● The new UK Intelligence Assessment Academy was opened in October 2019 and began to deliver a full curriculum of courses. The Academy switched to entirely virtual training with the onset of social distancing measures in March 2020.
COVID-19 impact	
In the first quarter of 2020, JIO produced several assessments on the COVID-19 pandemic, sharing these with a broader readership than usual, including the Department for Health and Social Care. The introduction of social distancing rules reduced the number of analysts that could work on high-side assessments. There was a reorganisation of staff to provide support to the Government's COVID-19 response.[45]	

[43] Figures previously indicated as falling under the Professional Head of Intelligence Assessment, and counted as 'corporate services' are now counted as 'operational activity'.

[44] Major achievements for 2018/19 were published in the Committee's Annual Report 2018–2019.

[45] Taken from JIO consolidated Quarterly Reports to the ISC (January–March 2020 and April–June 2020).

Homeland Security Group

Expenditure in 2018/19[46]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	896,600	119,400	1,016,000
Outturn	927,100[47]	112,200	1,039,300

Expenditure by category

- Grants spending: £787.9m
- Staff pay: £42m
- Other costs: £76.2m
- Against this, Homeland Security Group received an income of £19.5m[48]

Expenditure in 2019/20[49]

Total budget and outturn

£'000	Resource spending	Capital spending	TOTAL
Budget	1,003,200	104,300	1,107,500
Outturn	1,005,100[50]	104,900	1,111,000

Expenditure by category

- Grants spending: £867m[51]
- Staff pay: £52.2m[52]
- Other costs: £94.6m
- Against this, Homeland Security Group received an income of £18.7m

Administration

Staff numbers[53]

	Total staff	SCS	Non-SCS
31 March 2018	724	29	695
31 March 2019	722	22	700
31 March 2020	792	23	769

Recruitment in 2018/19

- Homeland Security Group recruited 201 staff in 2018/19 compared with 157 employees in 2017/18 against a target of 53 FTE. There was no recruitment target set for 2018/19.

Recruitment in 2019/20

- Homeland Security Group recruited 166 staff in 2019/20.[54]

[46] As reported to the Committee in the Homeland Security Group end-year report for the 2018/19 financial year.

[47] Homeland Security Group resource overspend was agreed by Home Office finance and was a result of the increase in activity following the attempted murder of the Skripals.

[48] Homeland Security Group income was primarily from the Asset Recovery Incentivisation Scheme which was moved into the Serious and Organised Crime Group.

[49] As reported to the Committee in the Homeland Security Group end-year report for the 2019/20 financial year.

[50] Homeland Security Group small resource and capital overspends were approved by Home Office finance and were offset against known underspends elsewhere in the department.

[51] The vast majority of Homeland Security Group expenditure is administered via grants mechanisms, and counter-terrorism policing grants constitute nearly 80% of Homeland Security Group's net budget. This figure largely reflects the £59m year-on-year increase in counter-terrorism policing grant.

[52] Part of the increase from 2018/19 is the full establishment of the Office for Communications Data Authorisation (OCDA) during 2019/20, which has a large staffing element (over 100 FTE).

[53] These figures refer to the number of FTE 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 2019/20 of just under £2m. Figures provided from 2019/20 Homeland Security Group snapshot. Homeland Security Group does not have any specific recruitment targets but aims to recruit staff to fill vacancies that arise during the financial year. On average, the churn rate of staff is 15%.

[54] Figures provided from 2019/20 Homeland Security Group snapshot. Homeland Security Group does not have any specific recruitment targets but aims to recruit staff to fill vacancies that arise during the financial year. On average, the churn rate of staff is 15%.

Major projects in 2018/19	● None reported.
Major projects in 2019/20	● None reported.[55]
Diversity and inclusion 2018/19	● Work is being carried out on a refreshed Diversity and Inclusion Strategy to prioritise and focus efforts on tackling notable under-representation. ● Appointment of a new Director-level senior sponsor leading on Diversity and Inclusion across Homeland Security Group. ● Homeland Security Group has collaborated closely with MI5 on trans visibility, and a number of workshops and bespoke trans awareness training packages have been launched.
Diversity and inclusion 2019/20	● A refreshed Homeland Security Group Diversity and Inclusion Action was launched in October 2019. ● Homeland Security Group has mandated unconscious bias training for all senior colleagues in order for staff to take part in interview panels for Homeland Security Group roles. ● A Career Watch Sponsorship programme for BAME and disabled employees was launched. ● Work is being carried out on reviewing Homeland Security Group leadership and management training in order to ensure a more inclusive working environment. ● Diversity and Inclusion leads held a number of cross-team discussions on Windrush and Black Lives Matter, running surveys and listening circles for BAME staff to understand their lived experiences and what support they would like to help them progress. Also planned are Let's Talk About Race sessions. This has informed Homeland Security Group's new Diversity and Inclusion Action Plan.
Allocation of effort at 31 March 2019	● National Security Directorate – 34% ● PREVENT and Research and Information Communication Unit – 18% ● PROTECT PREPARE (CBRNE) and science and technology – 17% ● Chief Operating Officer's directorate (including Communications Data Lawful Intercept, Planning and Resources Unit and the Joint Security and Resilience Centre) – 18% ● CONTEST (formerly known as Strategy, Planning and International) – 13%
Allocation of effort at 31 March 2020	● National Security Directorate – 37% ● PREVENT and Research and Information Communication Unit – 19% ● PROTECT PREPARE (CBRNE) and science and technology – 16% ● 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) – 11%

[55] Homeland Security Group has highlighted in previous returns that the Communications Capabilities Development (CCD) programme transitioned from a programme into the Communications Data and Lawful Intercept (CDLI) service partnership on 1 April 2018. Therefore, Homeland Security Group is no longer running any major project defined by the Infrastructure and Projects Authority's Government Major Projects Portfolio (GMPP).

Major achievements reported to the Committee for 2019/20[56]	● Co-ordinated the government response to the attack in Reading in June 2020. ● Proscription of a number of Extreme Right-Wing terrorist groups. ● Announced plans for a new world-leading Counter-Terrorism Operations Centre (CTOC) bringing together the Intelligence Community, counter-terrorism policing, government departments and the criminal justice system in one place. ● Published the full government response to the Online Harms white paper in December 2020 (in conjunction with the Department for Digital, Culture, Media and Sport). Interim codes of practice for terrorist and child sexual exploitation and abuse content and activity were published that have been developed in conjunction with law enforcement and the Intelligence Community. ● The UK–US Bilateral Data Access Agreement completed its US congressional review period, enabling the exchange of diplomatic notes. A draft Statutory Instrument was also laid before Parliament to enable formal oversight by the Investigatory Powers Commissioner's Office.

COVID-19 impact[57]

Towards the end of the 2019/20 financial year, the COVID-19 pandemic had a significant impact on Homeland Security Group's working practices and output.

In March 2020, all Homeland Security Group staff were required to work from home unless they were undertaking a critical function that could only be carried out in the office. This significantly reduced the number of staff going into Homeland Security Group offices and working on Top Secret systems.

PREVENT's online policy unit worked with Five Eyes partners on a COVID-19 analytical framework to determine the impact of COVID-19 on online radicalisation and, where required, how governments and technology companies should adjust their responses as a result.

[56] Major achievements for 2018/19 were published in the Committee's Annual Report 2018–2019.

[57] Taken from Homeland Security Group consolidated Quarterly Reports to the ISC (January–June 2020).

E02696743
978-1-5286-3040-5