

IPCO

Investigatory Powers
Commissioner's Office

OCDA

Office for Communications
Data Authorisations

Annual Report of the Investigatory Powers Commissioner 2019

Annual Report of the Investigatory Powers Commissioner 2019

Presented to Parliament pursuant to Section 234(6)&(8) of the Investigatory Powers Act 2016

Ordered by the House of Commons to be printed on 15 December 2020

Laid before the Scottish Parliament by the Scottish Ministers 15 December 2020

HC 1039

SG/2020/164



© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at info@ipco.org.uk.

ISBN 978-1-5286-2123-6

CCS0820043340 12/20

Printed on paper containing 75% recycled fibre content minimum.

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

Contents

Letter to the Prime Minister	5
1. Introduction by the Investigatory Powers Commissioner, Sir Brian Leveson	6
2. Legal and Policy	8
3. Protecting confidential or privileged information	18
4. Communications and engagement	23
5. Office for Communications Data Authorisations (OCDA) processes and methodology	28
6. Office for Communications Data Authorisations (OCDA) observations	31
7. Inspection methodology	32
8. MI5	39
9. Secret Intelligence Service (SIS)	51
10. Government Communications Headquarters (GCHQ)	62
11. Ministry of Defence	73
12. Law Enforcement Agencies and Police	76
13. Wider public authorities	97
14. Local authorities	104
15. Prisons	111
16. Warrant Granting Departments	117
17. Technology Advisory Panel	120
18. Errors and breaches	124
19. Statistics	138

Annex A: Glossary of Authorities	148
Annex B: Budget	150
Annex C: Serious Errors	151
Annex D: Communications Data	161
Annex E: Public Engagements	165

Letter to the Prime Minister

The Rt Hon. Boris Johnson MP
Prime Minister
10 Downing Street
London
SW1A 2AA

October 2020

Dear Prime Minister,

I enclose the Annual Report covering the work of the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) from 1 January to 31 December 2019.

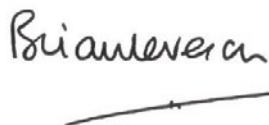
This is my second report to you as the Investigatory Powers Commissioner. It covers both the final months of oversight under my predecessor, The Rt Hon. Lord Justice Fulford, and my initial period as Commissioner. This report, as those before it, has been written in two sections. This public section includes information on the use of covert powers by UK authorities and includes the details required of me under section 234 of the Investigatory Powers Act 2016. The second section, the Confidential Annex, contains sensitive details the publication of which may be prejudicial to the public interest.

For the first time I have included details of the work of OCDA, which was established in 2018 under the Investigatory Powers Act and also falls under my responsibility. I have been impressed by the tremendous effort that has gone into setting up the office, from both the staff within the new organisation and from those with whom we work, in particular the Home Office. OCDA is now delivering independent decisions on communications data applications and has already demonstrated the value of this approach for both transparency and compliance.

It is for you to determine, in consultation with my office, whether this report can be published in its full form, without releasing material which would be contrary to the public interest, or prejudicial to national security, to the prevention or detection of serious crime, to the economic wellbeing of the United Kingdom, or to the discharge of the functions of those authorities which I oversee.

In my first months as Commissioner, I have been struck by the dedication and professionalism of all the representatives I have met from the authorities I oversee as they undertake vital work within the increasing challenges of modern society. I have been particularly impressed with the openness with which I have been received and the support I have been given in my ambition to increase the transparency with which this work is conducted, despite the obvious need to safeguard sensitive operations and national security.

Yours sincerely,



The Rt Hon. Sir Brian Leveson
The Investigatory Powers Commissioner

1. Introduction by the Investigatory Powers Commissioner, Sir Brian Leveson

I am delighted to present what is, in reality, my first Annual Report as Investigatory Powers Commissioner (IPC). As required by section 234 of the Investigatory Powers Act 2016 (IPA), the Report sets out details of the how the functions of the Judicial Commissioners were carried out during 2019. I have also chosen, although not obliged by legislation, to provide additional information on the activities of the Office for Communications Data Authorisations (OCDA), which also operates under the jurisdiction of the IPC. OCDA makes decisions on whether to grant or refuse communications data requests and, in the process, ensures that all requests are lawful, necessary and proportionate; it became fully functional during the course of 2019.

After my appointment in October 2019, I was responsible for despatching the annual report for 2018 which reported on the work of IPCO during the stewardship of the Rt. Hon. Sir Adrian Fulford. To a very large extent, the activity outlined in this report also took place when he was the IPC. I acknowledged his work last year but repeat that we owe him a real debt of gratitude: he left both IPCO and OCDA in a very strong position.

The operation of the 2016 Act was an entirely new area of work for me and I have found my first few months in the role tremendously interesting. I must also report that I have been very impressed by the energy and commitment of the Judicial Commissioners, the members of the Technology Advisory Panel and all of the staff at IPCO and OCDA. I am confident that, together, we can continue to provide a very high standard of scrutiny and oversight to ensure that the use of covert powers by the UK fully complies with its human rights obligations.

On the whole, I have also been impressed by the high level of compliance with the legislation and relevant Codes of Practice. This can be seen both through the reports on the inspections of this activity and from the low proportion of errors that are reported. Having said that, however, we have seen two large scale errors during the year, one at MI5 and one at HMRC. Both of these led to focused inspection work by IPCO and are addressed in greater detail in Chapters 8, 12 and 18 of this report. Such errors highlight the importance of continued vigilance in the face of change and of embedding strong compliance cultures across public authorities exercising intrusive powers. I am very pleased that both organisations recognised the gravity of the issues that were uncovered and both have addressed them in a comprehensive way.

In response to the issues which arose in MI5, IPCO has instigated a thorough review of data assurance across all of the public authorities we oversee. The aim of the review is to ensure that responsibilities for data handling, retention and destruction properly are understood across all public authorities and that, where necessary, actions are in train to ensure those responsibilities are being met. This is a major piece of work which was originally expected to take between 18 months and two years. You can find more information on the approach that is being taken later in this report.

The overall structure of the report is much the same as last year. As I have indicated, there are new sections covering the work of OCDA this year and the separate chapter on the Consolidated Guidance has been removed. Instead, oversight of this activity is now addressed in the chapters relating to the relevant agencies, where it more logically sits alongside other powers. Last year, we set out some of the challenges we had received from an NGO in relation to the absence of statistics on the operation of the Consolidated Guidance. This year, I am pleased that it has been possible to agree that some data should be published although I underline the very clear caveats which surround the figures. This material can be found in Chapter 19.

Whilst the focus of this report is appropriately on what happened in 2019, it is important to take this opportunity to mention the impact of the COVID-19 pandemic on the work of IPCO and OCDA in 2020. The need to change our ways of working, almost overnight, has led to some imaginative thinking about how we can meet our statutory functions in different ways, particularly as, for obvious reasons, we had to suspend our normal programme of face to face inspections in March. We have been able to trial a number of different formats for remote inspections and, although it will continue to be important for inspection visits to be able to take place in person, I hope that we will be able to apply at least some of this innovation for the longer-term.

Fortunately, Parliament swiftly enacted some important provisions for IPCO in the Coronavirus Act 2020. As a result, I was able to appoint a number of temporary Judicial Commissioners who were all under the age of 70 and, therefore, not subject to the same lockdown restrictions as almost all of the original cohort of Judicial Commissioners. I am very grateful to them (and to Sir Adrian Fulford whom the Prime Minister also re-appointed as a Judicial Commissioner) for putting themselves forward for this additional work; their commitment has ensured that the authorisation process has continued unabated during this period.

I am also very grateful to all of those in IPCO and OCDA who continued to attend the office to ensure that our critical work was done, and to those who adjusted their ways of working to ensure that we have been able to continue to meet our statutory functions while working from home. This has not been easy for anyone, but I have been impressed by the commitment across both teams, many of whom were also juggling caring and other responsibilities at the same time.

The impact of COVID-19 on public authorities also means that it is likely that they will make slower progress in addressing our previous recommendations many of which are discussed in this report. The aspirations expressed in relation to our inspections and other activities have also been affected. Suffice to say that we will continue to monitor progress closely and will return to the impact of the pandemic and the necessary consequential changes to our practices in the 2020 Annual Report.

2. Legal and Policy

Overview

- 2.1 Legal and policy issues continue to be a key focus for the Investigatory Powers Commissioner (IPC). The powers that the Investigatory Powers Commissioner's Office (IPCO) oversees, and upon which the Office for Communications Data Authorisations (OCDA) takes decisions, can all be subject to direct and indirect challenge in the UK and European courts. The legal teams of both IPCO and OCDA monitor litigation that may affect the Commissioner's oversight role and the IPC is committed to providing such assistance as the courts or Investigatory Powers Tribunal (IPT) may reasonably require of him.
- 2.2 This chapter gives an overview of:
- the key legal and policy developments that have impacted on IPCO and OCDA in 2019; and
 - legal and policy approaches and decisions that we have taken on particular topics relevant to the IPC's functions.

Legal and policy developments relevant to our work

Ongoing implementation of the Investigatory Powers Act 2016 (IPA)

- 2.3 For the IPC, the major impact of the ongoing implementation of the IPA arose from the commencement of section 60A which changed the regime for the authorisation of communications data (CD) requests. Implementation of these provisions was staggered over the course of the year for different public authorities. This has meant that by the end of the year, all non-urgent authorisations for CD (other than those relating to national security), are now authorised by the IPC under delegated powers.¹
- 2.4 The IPC discharges this function through delegating decision-making to "authorising individuals" in OCDA. OCDA is an administratively separate office to IPCO, and its work over the course of 2019 is set out in more detail in Chapters 5 and 6. Chapter 19 also provides statistics in relation to the number of CD authorisations granted by OCDA.
- 2.5 Section 77 of the IPA requires that any CD authorisation intended to identify or confirm a source of journalistic information requires prior approval by a Judicial Commissioner. This section came into force in 2019 and applies for all authorisations other than those which relate to an imminent threat to life. This provision, under 77(1)(b), allows for emergency requests to be made without prior judicial approval. Further details on the protections in relation to journalists and journalistic sources are given in Chapter 3.

1 Statistics on the use of communications data, including routine and urgent applications are given in the relevant chapters for each type of authority, and in Chapter 19 which covers Statistics.

Table 1: Dates of transition to the Investigatory Powers Act 2016 (IPA)

Date (2019)	Provision
27 February, 15 March; and 22 March	UK intelligence community transition to the IPA for communications data
26 March	OCDA commenced independent authorisation operations
26 March	The first wider public authority transitioned to the IPA
8 May	The first phase of transition for police and law enforcement agencies (LEA) was completed by the East Midlands region
June to October	The remainder of the LEA sector completed a phased transition to the IPA
19 November	The final transition was completed by the Metropolitan Police Service

Schedule 3 of the Counter-Terrorism and Border Security Act 2019

- 2.6 Schedule 3 of the Counter-Terrorism and Border Security Act 2019 (CTBS Act) provides the IPC with a function in relation to “port stops” that are undertaken for the purposes of determining whether a person appears to be engaged in hostile activity. Hostile activity includes conduct that threatens national security or the economic wellbeing of the United Kingdom, where this is carried out for or on behalf of another state, or in the interests of another state.
- 2.7 Under Schedule 3, examining officers may, for example, retain an article at a port if they believe that the article could be used for the carrying out of a hostile act. An example of this might be an item that officers have seized from a person who is entering or leaving the UK. In that event, the IPC must be informed of the retention of the article and the IPC must then determine whether the retention should continue – i.e. whether there are reasonable grounds for believing that the article could be used in connection with a hostile act. The IPC will invite written representations from the person concerned, as well as from the police and the Secretary of State, before making a decision regarding the retention and any proposed use of the article.
- 2.8 Alternatively, having examined an article, an examining officer may seek to simply retain a copy of it instead under Schedule 3. If the copy includes confidential material then the IPC must be notified. The IPC must determine whether or not to authorise the retention and use of that copy in the interests of, for example: national security, the prevention or detection of serious crime or to prevent death or significant injury. Again, the IPC will invite written representations from the affected parties before making a decision.
- 2.9 The Home Office carried out a public consultation, during 2019, on the draft Code of Practice for Schedule 3 and IPCO contributed to that consultation. Schedule 3 came into force in June 2020.
- 2.10 As well as having a role in making determinations under Schedule 3, the IPC will also keep the use of Schedule 3 powers under review. He will report annually to the Home Secretary on the use of these powers.

Big Brother Watch – claim to the European Court of Human Rights

- 2.11 In our 2018 report, we summarised the judgment made by the European Court of Human Rights (ECtHR) in relation to *Big Brother Watch v UK* ('the BBW judgment').² We noted that we had been working with the Government to understand their response to the judgment and that they had proposed that, where an intelligence service intended to select secondary data (such as communications data) for examination³ in relation to an individual known to be in the British Islands, it would be beneficial for the examination to be certified as necessary and proportionate by the Secretary of State. Details of how this has been inspected are given in Chapter 10, which covers our oversight of the Government Communications Headquarters (GCHQ).
- 2.12 The Grand Chamber of the ECtHR heard the appeal from the decision of the First Section in July 2019 and its ruling is currently awaited.

Liberty's judicial review challenge to the Investigatory Powers Act

- 2.13 On 29 July 2019, the High Court delivered its second judgment in the case of *Liberty v Secretary of State for the Home Department* [2019] EWHC 2057. In its first judgment in this case, in 2018, the High Court had ruled in relation to the compatibility of Part 4 of the IPA (retention of communications data by telecommunications operators) with EU law.
- 2.14 In its judgment of July 2019, the High Court ruled in relation to Liberty's challenge to the IPA brought under the Human Rights Act. Liberty (with the National Union of Journalists as interveners) contended that various Parts of the IPA, and in particular the bulk powers regimes, were incompatible with the European Convention on Human Rights (ECHR). Liberty's challenge related to:
- bulk interception warrants (Part 6, Chapter 1 of the IPA);
 - bulk and thematic equipment interference warrants (Part 6, Chapter 3 and Part 5 of the IPA);
 - bulk personal datasets (Part 7 of the IPA);
 - bulk communications data (Part 6, Chapter 2 of the IPA); and
 - acquisition and retention of communications data (Parts 3 and 4 of the IPA) and contended that those Parts of the IPA:
 1. were incompatible with Articles 8 and 10 of the ECHR; and
 2. provide insufficient safeguards for lawyer-client communications and journalistic material (including confidential sources of journalistic information).
- 2.15 Further questions as to the compatibility of the bulk powers with EU law have been left for determination in due course. Of particular relevance to this will be the awaited ruling of the European Court of Justice in relation to the referral to that Court, by the IPT,⁴ of various questions in relation to the acquisition of bulk communications data under section 94 of

2 European Court of Human Rights, "Q&A on the judgment *Big Brother Watch and Others v. United Kingdom*" (13 September 2018), https://www.echr.coe.int/Documents/Press_Q_A_Brother_Watch_ENG.pdf

3 An examination being the act of material being read, looked at or listened to by the persons to whom it becomes available as a result of a warrant.

4 See *Privacy International v Secretary of State for Foreign and Commonwealth Affairs (No.2) Note* [2017] UKIPTrib 15_110-CH

the Telecommunications Act 1984 (the predecessor regime to what is now Part 6, Chapter 2 of the IPA).

- 2.16 At the hearing in June 2019, the High Court also heard argument of, and considered matters relating to, failures by MI5 to comply with the handling arrangements for data acquired under IPA warrants. In chapter 8 of this report, we describe in detail the serious compliance failings by MI5 in its handling of data obtained under IPA and Regulation of Investigatory Powers Act 2000 (RIPA) warrants. In particular, we have described:
- the inspections carried out by IPCO to investigate these compliance issues; and
 - the IPC's decision (of 5 April 2019) when he approved the issue of a number of warrants to MI5, on the basis of the steps that MI5 had, by then, taken to rectify the most immediately pressing issues relating to the safeguarding of IPA warranted material.
- 2.17 In its judgment of 29 July 2019, the High Court determined the ECHR compatibility of the IPA against the background of the First Section's judgment in the BBW case; it being recognised that the Grand Chamber's ruling in the BBW case (when that is provided) might have implications for any appeal from the High Court's judgment. The High Court rejected the claim for judicial review concluding that:
- in principle, bulk powers are compatible with the ECHR; and
 - the IPA contains sufficient safeguards to avoid the risk of abuse of power and in order to be in accordance with law.
- 2.18 In the course of its judgment, the High Court considered the MI5 compliance issues, the actions taken by IPCO, and the view reached by the IPC in relation to MI5 warrants. The Court declined to rule on whether or not MI5 had complied with the requirements of the law, concluding that that question was different to that which it had to determine in the judicial review where the issue was the ECHR compatibility of the legislative scheme. The High Court noted that these issues as to compliance might be the subject of future litigation, potentially before the IPT. This transpired later in the year as described below.

Assistance to the Investigatory Powers Tribunal (IPT)

- 2.19 IPCO has a statutory obligation to assist the Investigatory Powers Tribunal (IPT), further to section 232(1) of the IPA. During the course of 2019 we provided information to the IPT, in response to requests for assistance, as follows:
- c. For the purposes of the "Third Direction" litigation (see below) we provided information to the IPT in relation to the IPC's oversight under the Prime Minister's direction of 22 August 2017.
 - d. For the purposes of a complaint to the IPT, by an individual in relation to a police force, the IPT sought assistance in verifying the police force's assertion that, following searches carried out by it, it did not hold any relevant information. Our Inspectors attended the police force's offices, interviewed staff and reviewed the force's records before providing a report to the IPT on their findings.

Privacy International's (and others') challenge, in the IPT, in relation to MI5's policy on agents who participate in crime – the "Third Direction" litigation

- 2.20 In proceedings in the IPT, Privacy International (together with Reprieve, the Committee on the Administration of Justice and the Pat Finucane Centre) challenged the lawfulness of MI5's policy relating to agents who participate in crime. In particular, the claimants challenged the lawful basis for such a policy and whether the policy was compatible with the ECHR.
- 2.21 Further to a direction issued by the Prime Minister on 22 August 2017, the IPC is required to *"keep under review the application of [MI5] guidelines on the use of agents who participate in criminality and the authorisations issued in accordance with them."* MI5's "authorisations" do not, in fact, purport to authorise criminality, in the sense of providing any form of immunity from prosecution. Rather, the authorisations are intended to explain and justify the decision to engage in criminality and, in particular, the public interest in doing so. Those reasons can then, if required, be provided to prosecutors.
- 2.22 The IPT ruled, on 20 December 2019 (following a hearing in November 2019) that MI5 does have the power, as a matter of public law, to engage in activities which may involve their agents participating in crime. The IPT also concluded that the oversight powers, given to the IPC, *"do provide adequate safeguards against the risk of abuse of discretionary power."* The IPT also rejected the arguments that the policy was incompatible with the ECHR. The claimants applied for, and were granted, permission to appeal to the Court of Appeal from the IPT's ruling; a hearing before the Court of Appeal is expected to take place during the course of 2020.
- 2.23 IPCO's oversight of MI5's activities in relation to agents who participate in crime is described in Chapter 8 of this report.

Liberty and Privacy International claim, in the IPT, arising from the MI5 compliance issues

- 2.24 In February 2020, Liberty and Privacy International brought a new claim (and an amendment to their existing claim relating to bulk data) against the Home Office and MI5 in relation to the MI5 compliance issues that were considered by the IPC during 2019, as referred to by the High Court in Liberty's judicial review of the IPA (as mentioned above).
- 2.25 The IPC will provide such assistance to the IPT as may be required in these proceedings.

Review of the Consolidated Guidance

- 2.26 The 2018 report set out details of the IPC's role in the Government's 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 Consolidated Guidance). In brief, the Prime Minister invited the IPC *'to make proposals to the Government about how the Guidance could be improved, taking account of the [Intelligence and Security Committee of Parliament] ISC's views and those of civil society'*. Nine written submissions were received in response to a public consultation,⁵ from Non-Governmental Organisations (NGOs), academics and from Her Majesty's

5 IPCO, "Consultation on the Consolidated Guidance" (April 2018), <https://ipco.org.uk/docs/IPCO%20Consultation%20on%20the%20Consolidated%20Guidance.pdf>

Government (HMG).⁶ On 12 December 2018, Lord Anderson of Ipswich KBE QC hosted an invitation-only event at Chatham House on behalf of the IPC for some of those who had responded or had a particular interest in this area. The event enabled detailed exploration of the central points raised in the responses.

- 2.27 Following this process, and extensive consultation with the relevant agencies on the practical implications of proposed amendments, the IPC, Sir Adrian Fulford, submitted his recommendations to the Prime Minister on 12 June 2019. These have now been accepted in full.⁷ The new *'Principles relating to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees'* (The Principles) were published by the Government on 18 July 2019.⁸ The Principles took effect from 1 January 2020. On 13 December 2019 the Prime Minister directed the IPC to keep under review compliance with The Principles by the intelligence agencies, Her Majesty's Armed Forces and the Ministry of Defence, the Metropolitan Police and the NCA. We will provide a full report on the first year of operation of The Principles in our 2020 Annual Report.

Third Party Data

- 2.28 In 2019, we discussed the scope of Part 7 of the IPA (bulk personal datasets) with UKIC with particular reference to data held by third parties. In general, any access which UKIC has to personal data held by third parties does not require authorisation under Part 7 of the IPA, because UKIC is not "retaining" the data within the meaning of section 199 of the IPA. The consequence of this is that, for a dataset which would otherwise meet the definition of a BPD in section 199 of the Act were it to be retained by UKIC (i.e. it relates to a large number of individuals, the majority of whom are not of intelligence interest, and it is held electronically for analysis), Part 7 of the IPA does not apply if the dataset is in fact retained by a third party within the meaning of section 199. Instead, UKIC rely on their core statutory functions in the Security Service and Intelligence Services Acts respectively, together with the statutory information gateway in section 19 of the Counter-Terrorism Act 2008, to access such datasets.
- 2.29 In light of the scope of Part 7 of the IPA, we conducted an extensive review of bulk datasets held by third parties to which UKIC had access in order to provide assurance that BPD warrants were being obtained where applicable. Given that the processing of data held by third parties falls outside our oversight functions, we focused on whether UKIC was compliant with the requirements of Part 7 of the IPA. We concluded, in the case of the datasets examined by the review, that UKIC's access was not in breach of the requirements of Part 7. However, we will continue to keep under review UKIC's compliance with Part 7 in this regard. Whilst UKIC access to data held by third parties is not currently subject to oversight by IPCO, we have recommended that HMG consider bringing it within IPCO's oversight functions.

6 IPCO, "Consultations" (October 2018), <<https://ipco.org.uk/default.aspx?mid=13.11>>

7 Prime Minister, "Review of the Consolidated Guidance" (18 July 2019), <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2019-07-18/HCW51738/>

8 Her Majesty's Government, "The Principles" (July 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818306/20190718_The_Principles_relating_to_the_detention_and_interviewing_of_detainees_overseas.pdf

Judicial engagement on authorisation matters

- 2.30 During 2019 we have continued to benefit from a wide range of discussions on emerging issues with those we oversee. We held four quarterly meetings of the Judicial Commissioners (JCs), during which they were briefed by representatives from the UK intelligence community (UKIC), law enforcement, HMG and members of the Technology Advisory Panel (TAP) on the present intelligence and law enforcement threats, technological or operational developments, and litigation and other legal developments relevant to our work.
- 2.31 The JCs regularly seek additional information about applications for warrants before making a decision on them. On occasion, a request for additional information or clarification may result in the withdrawal of an application by the warrant requesting body. The IPC considers the withdrawal of an application, in response to a request for information or clarification, as an example of the value of judicial oversight and challenge.
- 2.32 The IPC and the JCs have also continued to encourage briefings from law enforcement bodies and UKIC well in advance of receiving novel or contentious applications. This kind of engagement means that JCs or IPCO subject-matter experts can provide a non-binding view on matters relevant to a warrant application, so that these can be addressed in the application as then formally submitted.

Definition: the double lock

The “double lock” is the process by which a Judicial Commissioner (JC) must review and authorise an application to use certain intrusive investigatory powers. It is a mechanism to seek prior approval. This means that, following Secretary of State authorisation, a warrant under the Investigatory Powers Act 2016 cannot be issued until it has been approved by a JC.

Thematic warrant applications

- 2.33 During the course of 2019, the JCs refused a number of thematic warrant applications from a range of law enforcement agencies for targeted equipment interference and sought further information and clarification from the forces regarding others. The refusal of these warrants in general did not result from inappropriate use of powers or suggest that the proposed actions were not necessary. However, the JCs were keen to ensure that the legal documentation of the requests (the application) were correct and consistent between forces. The Commissioners identified the following concerns with some applications for thematic warrants:
- they included a general description of subjects in circumstances where it was not clear why it was not reasonably practicable to include the names/descriptions of such persons; and/or
 - they provided an insufficient explanation as to the necessity and proportionality for including as subjects those persons who were described by reference to a general description.
- 2.34 Throughout the year, we found that similar issues were arising across the country, so our Inspectors and legal team engaged with:
- lead individuals in the law enforcement agencies concerned, with a view to ensuring that the JC's concerns/points were disseminated appropriately; and

- key national leads on equipment interference, in order to assist law enforcement bodies more generally to better understand the thematic warrant requirements as set out in the IPA and the Code of Practice for Equipment Interference.

Definition: Thematic warrants

Thematic warrants are warrants that have more than one subject. There are two types of thematic warrant:

- The first individually names/describes all the subjects. Any additional subjects can only be added by a modification. For law enforcement bodies these require prior approval by a Judicial Commissioner, or retrospective approval if the modification is urgent.
- The second does not individually name/describe each subject, because this is not reasonably practicable. In relation to this second type of warrant, the authority does not need to add subjects by modification: action may be taken against a person, organisation or piece of equipment (depending on the type of thematic warrant in question) falling within the general description of the subjects.

Example: Thematic warrants

An example of such a general description could be *“members of the media wing of a [named] terrorist organisation”*.

If such a description was used in a thematic warrant covering a group of persons which shares a common purpose, the authority could conduct specific actions authorised under the warrant against members of that organisation, although they have not been individually named on the warrant, as long as they are assessed to be members of the organisation named on the warrant. The Codes of Practice give guidance as to the circumstances in which it may be appropriate to provide a general description of the subjects of the warrant.

- 2.35 JCs will continue to scrutinise applications and renewals for thematic warrants. Our inspections in 2020 will focus on thematic warrants, both in relation to modifications that are made to them and the activity conducted by the force. This process will give us a good level of assurance that the thematic provisions are being used well and appropriately throughout law enforcement.

Appeals to the IPC

- 2.36 If a JC refuses to approve the application for a warrant, the requesting authority may ask the IPC to review the decision and decide whether to overturn the refusal. During 2019 there were no appeals to the IPC in relation to refusals by a JC of a warrant application.

Technical capability notices (TCNs), national security notices (NSNs), and communications data retention notices

- 2.37 The IPA introduced the power for the Secretary of State to issue notices to communications service providers and UK companies to assist public bodies and agencies working under the Act. These provisions consolidated existing arrangements and established a clear mechanism for authorising this activity. The JCs perform the double lock function, ensuring that each notice given is necessary and the actions required of the company or operator are proportionate to the stated aims of the work.

Definition: Technical Capability Notices (TCNs)

Under section 253 of the Investigatory Powers Act 2016, the Secretary of State, with approval from a Judicial Commissioner, may use TCNs to give telecommunications or postal operators notice of the requirement to have the capability to provide assistance with interception, equipment interference and the acquisition of bulk communications data (BCD). After a TCN has been issued and implemented, a company can act quickly and securely when a warrant is authorised.

Definition: National Security Notices (NSNs)

Under section 252 of the Investigatory Powers Act 2016, a Secretary of State, with approval from a Judicial Commissioner, can use an NSN to direct a UK telecommunications operator to act in the interests of national security. This covers actions to assist the security and intelligence agencies, which may be additionally authorised under a warrant. NSNs could, for example, ask a company to provide access to a particular facility.

- 2.38 As in previous years the Technology Advisory Panel (TAP) assisted the JCs in considering TCNs and NSNs that were approved in 2019. The TAP provided briefings, covering technical detail and practical processes, to the JCs to assist in their consideration of these applications.

Communications data retention notices

- 2.39 In July 2019 a JC provided the first approval of a CD retention notice regarding internet connection records (ICRs) relating to a telecommunication operator. This approval was granted solely for the purposes of a trial, ('live' authorisations and acquisition of ICRs), being conducted by law enforcement in conjunction with the Home Office, of systems and processes for the proposed future operational use of ICRs. An ICR is a record of an event, held by a telecommunications operator, about the sites or services to which a subject has connected on the internet – but explicitly not what was done on those sites or services (the content). As part of the same trial, although solely for testing purposes at this stage (no 'live' authorisations and no acquisition of ICRs by a relevant public authority), in October 2019 a JC approved a further CD retention notice regarding ICRs relating to a different telecommunications operator.
- 2.40 The JC sought and received advice from the TAP, as part of his consideration of these two applications for the retention of ICRs.

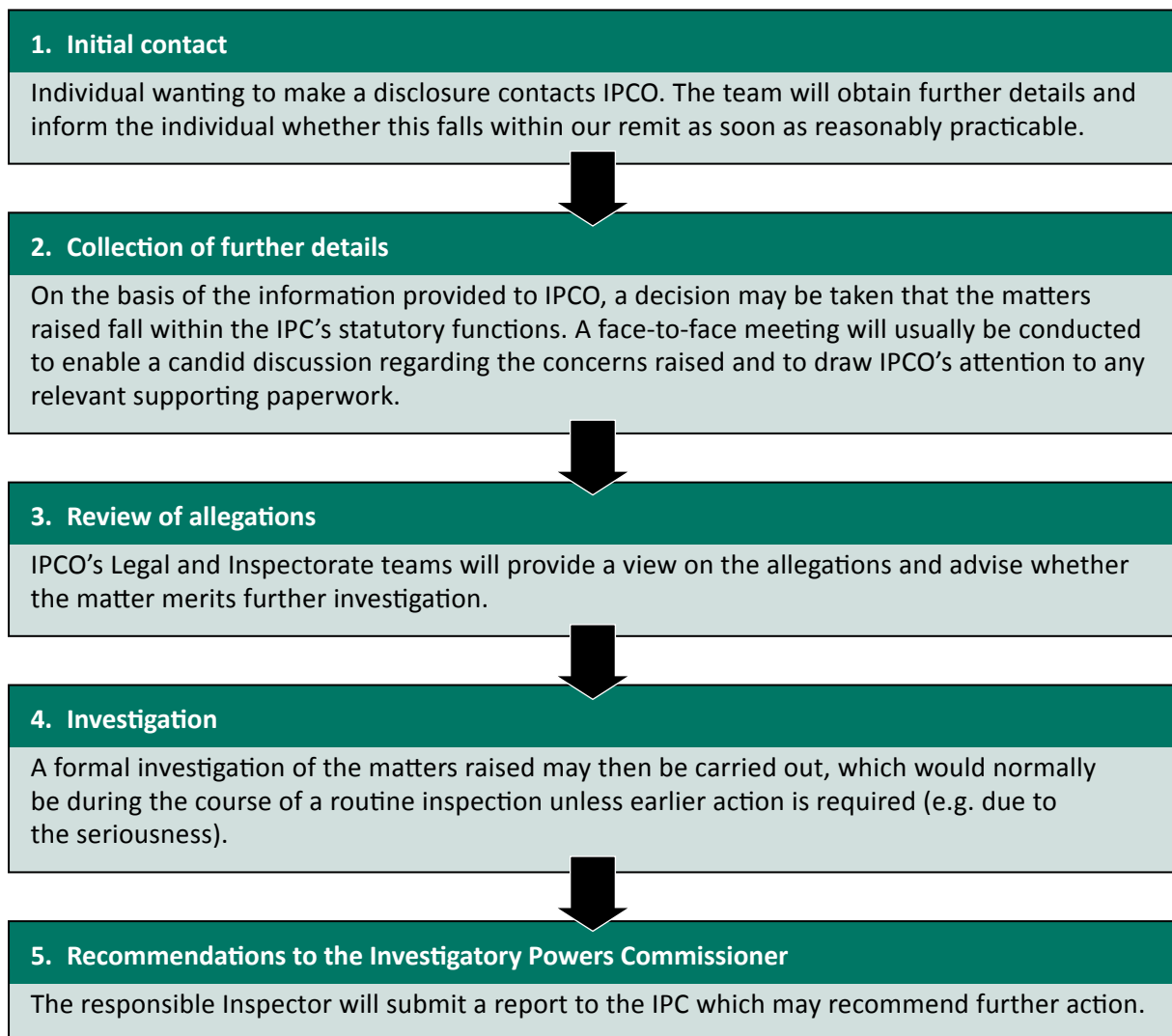
Definition: communications data retention notices

Section 87 of the Investigatory Powers Act 2016 gives the Secretary of State the power to give a data retention notice to a telecommunications operator or postal operator, requiring them to retain relevant communications data (CD) for a maximum of 12 months, if it is considered necessary and proportionate for one or more statutory purpose. A notice to retain CD can only be given where the Secretary of State, having taken into account relevant information, considers it necessary and proportionate to do so and where the decision to do so has been approved by a Judicial Commissioner.

Raising Concerns with IPCO

2.41 Section 237 of the Act established an information gateway which provided for disclosures to the IPC or any JC. This provision provides an independent channel for individuals to raise concerns about the activities of their organisation. Disclosures of information relating to the use of investigatory powers can be made without the person breaching an obligation of confidence or any other restriction on the disclosure of information (with the exception of data protection legislation). Although it is important to note that IPCO does not perform an ombudsman role (such a function is properly that of the Investigatory Powers Tribunal), IPCO's statutory information gateway enables both current and former staff of the public authorities which we oversee to raise any serious concerns they have with us. Where it is assessed that such concerns have merit, these will thoroughly be investigated and appropriate action taken.

2.42 The process for making a disclosure to IPCO is as follows:



2.43 In 2019, three disclosures were made raising concerns with IPCO, all in relation to law enforcement agencies. In two of these cases, it was found that there was sufficient concern for IPCO to investigate further. Following investigation, however, it was decided no further action was necessary as the allegations could not be substantiated. The third case is still under investigation.

3. Protecting confidential or privileged information

Overview

- 3.1 The Investigatory Powers Act 2016 (IPA) provides enhanced protection for certain forms of confidential or privileged information and the Investigatory Powers Commissioner (IPC) has a statutory role in authorising and overseeing the acquisition and retention of such material. The IPA and Codes of Practice (CoP) introduce specific safeguards for confidential or privileged material. These safeguards enhance the provisions in the Regulation of Investigatory Powers Act 2000 (RIPA)⁹ to protect sensitive material.

Legal professional privilege (LPP)

- 3.2 Legal professional privilege protects the right to seek legal advice and conduct litigation confidentially. Material subject to legal privilege, which would include most conversations and written advice between an individual or organisation and a legal advisor or representative, are protected by specific safeguards in a combination of primary legislation and the IPA and Codes of Practice.
- 3.3 Authorities must inform IPCO if they think it is necessary to retain LPP material. The decision to do so is considered and approved, if appropriate, by a Judicial Commissioner (JC). In these circumstances, the material and proposed use and handling arrangements are considered in order to determine whether the public interest in retaining it outweighs the public interest in the confidentiality of the item.
- 3.4 In IPCO's 2018 Annual Report we noted an expectation that the number of LPP-related issues that would be brought to our attention would likely increase in 2019 because of changes in protections set out in both the 2018 CoP for Covert Surveillance and Property Interference and the CoP for Covert Human Intelligence Sources (CHIS). There were two requests in 2019 to task CHIS to obtain LPP material.

LPP oversight

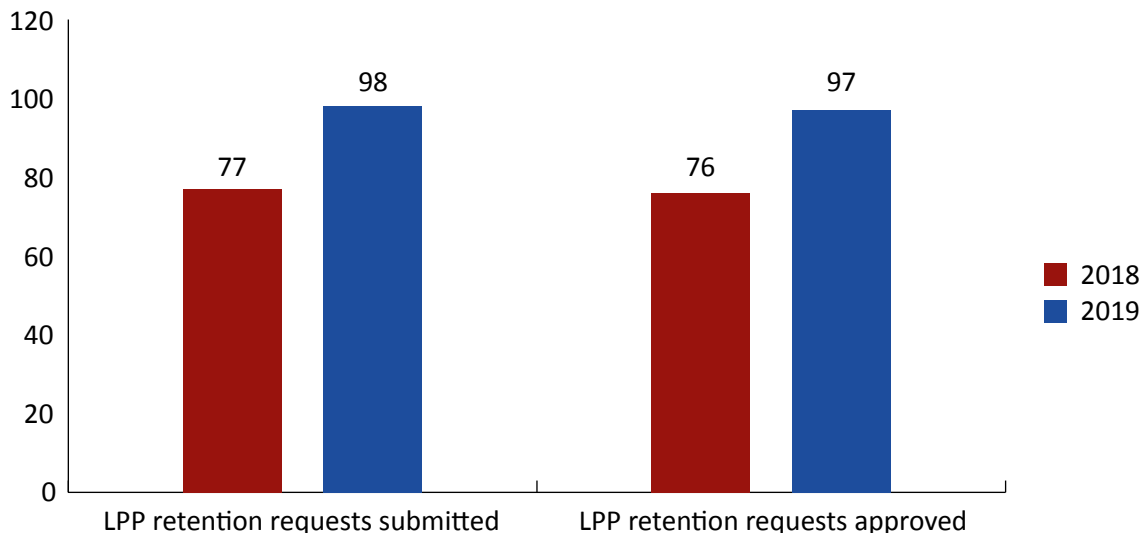
- 3.5 The requirement to safeguard LPP material is familiar to all of the authorities we oversee and as a result the level of compliance is generally good (see paragraph 12.31). Authorities continue to be cautious in their categorisation of LPP material and so we have a high level of confidence that material relating to legal advice is being properly handled.

9 The Regulation of Investigatory Powers (Scotland) Act (RIP(S)A 2000 regulates the use of surveillance and CHIS in Scotland.

Retention of items subject to legal professional privilege

3.6 A total of 98 applications were made to IPCO in relation to the retention of LPP material. Of those, 97 were approved.

Figure 1: Number of requests submitted and approved for LPP material in 2018 and 2019



Confidential journalistic material and sources of journalistic information

3.7 Confidential journalistic material and sources of journalistic information are also subject to specific safeguards to respect the freedom of the press. All applications made under the IPA and RIPA set out whether it is the purpose of the application to obtain confidential journalistic material or to identify sources of journalistic material and whether it is likely that such material will be obtained. Freedom of expression is protected under Article 10 of the European Convention on Human Rights (ECHR) and we would expect all relevant applications to consider the necessity and proportionality of any request in that context.

3.8 Our inspections have not identified any concerns in relation to the handling of any journalistic confidential material or material relating to journalistic sources. The casework flagged to us, and identified in this report, as relating to journalists can be split into three broad categories: those that relate to a journalist, those that relate to confidential journalistic material, and those that relate to journalistic sources.

3.9 The first of these is by far the most common, and it includes any communications data request that relates to a journalist. These requests are subject to an independent decision by the Office for Communications Data Authorisations (OCDA) and are not subject to JC review. We have continued to find that in the majority of cases the applications in this category relate to circumstances where a journalist has been a victim of crime which is under investigation, for example where a journalist has reported being the subject of harassment, and the police will make a request to capture their communications data records as evidence of this. Because of the safeguards in relation to this sensitive profession, we review a high proportion of this casework at our communications data inspections to ensure that the relevant considerations are well documented. In general, we have found this to be the case.

- 3.10 As shown at Annex D, 116 targeted communications data requests were made in relation to an individual of journalistic profession, whilst 15 were made to identify or confirm a journalistic source. More information is provided below in paragraph 3.14.
- 3.11 Numbers of authorisations in the second category, journalistic material, will always be substantially smaller and all applications have been subject to the double lock. As with other authorisations, it must be necessary and proportionate to conduct the proposed interference or interception and so the test that must be satisfied is no different. However, we expect additional consideration to be given to the sensitive material that may be obtained and to the public interest in safeguarding freedom of the press in order to satisfy the threshold in this context. We would also expect applications to give some consideration to how confidential material will be handled and the extent to which this material is expected to be relevant to the investigation.

Example: confidential journalistic material

For example, if a journalist was being investigated for their involvement in a serious crime, it may be necessary and proportionate to intercept the relevant communications but not necessary to review their professional communications other than to identify them and disregard them from the investigation.

We would therefore expect the intercepting agency to make provisions to disregard or dispose of that material for the duration of the interception. This would not be the case, however, if the journalist was using professional communications for the furtherance of serious crime.

- 3.12 Under RIPA Codes of Practice, applications to conduct surveillance and use CHIS where there is a likelihood of obtaining journalistic material must be subject to an additional level of internal scrutiny. The enhanced procedures for obtaining confidential information include requiring the request to be authorised at a more senior level. We would expect any relevant applications to include details of how this sensitive material will be protected.
- 3.13 In 2019, 17 applications were made for warrants under the IPA where the purpose was to obtain material which the intercepting agency believed would relate to confidential journalistic material. In all cases, the JCs were satisfied that the case for obtaining confidential material was well made and the proposed activity was necessary and proportionate. Only one application was made for the acquisition of communications data which was expected to include confidential journalistic material in 2019.
- 3.14 The third category relates to the identification of journalistic sources. Journalistic sources are protected in the IPA and we expect applications to identify these by to be rare. Applications relating to journalistic sources might either be for warrants, which would be considered by a JC, or for communications data under section 77 of the IPA, which will also be subject to judicial consideration. Under section 77, the JC must have consideration to the public interest in protecting a source of journalistic material. There was one warrant application to identify a journalistic source and 15 other applications were considered under section 77 in 2019.

Communications data requests relating to sensitive professions

- 3.15 In 2018, we noted that the statistics for applications relating to sensitive professions could be clearer and that we would work with the authorities we oversee to improve the presentation of these figures. We expect, based on the level of training received by these

individuals, that the applicant, Single Point of Contact (SPoC) and Authorising Officer (AO) will recognise and make reference to any sensitivities in the application. OCDA's central review function will improve consistency in this area and will mean that the IPC can have a high level of confidence that requests relating to sensitive professions are being correctly marked and handled appropriately in accordance with the CoP.

- 3.16 Throughout 2019, IPCO made suggestions to authorities that changes to workflow systems may help improve the accuracy of data. Inspectors will run specific free-text searches in relation to sensitive professions during inspections and so will review a high proportion of these applications. The most common issue we see is that a record is incorrectly marked as relating to a sensitive profession. Inspectors have found, that many such applications did not relate to a sensitive profession but were incorrectly marked as such because the 'N/A' option, which the applicant meant to select, sits directly above "journalist". The workflow providers have accepted our observation and we expect that they will improve the user interface for these systems to reduce mistakes of this kind.
- 3.17 In the future, ODCA will collate statistics in relation to sensitive professions for communications data (CD) applications so the figures published in this report will be gathered from a single central record. At OCDA, we will also continue to work with authorities to ensure that sensitive professions are marked correctly. OCDA staff, in line with advice from IPCO Inspectors, have encouraged applicants and SPoCs to think more widely about sensitive professions and to include, for example, community nurses and borough councillors. We anticipate that this guidance will encourage a more consistent approach, and therefore more accurate and comparable statistics.

Bulk authorisations

- 3.18 The nature of bulk acquisition means that material associated with journalists will be subject to collection in the same manner as all other individuals. The Act therefore provides a number of safeguards to ensure that bulk collection does not enable unnecessary retention or examination of confidential journalistic material.
- 3.19 Under Part 6 of the Act, an intelligence agency may apply for a bulk interception warrant (covered by Chapter 1) or equipment interference warrant (covered by Chapter 3). Sections 154 and 195 impose restrictions in relation to confidential material: the relevant agency must inform the IPC as soon as reasonably practicable if material containing confidential journalistic material is being retained for any purpose other than destruction.
- 3.20 The Act does not include specific safeguards in relation to journalists or confidential journalistic material for Bulk Personal Datasets (BPD). However, these are set out in the Codes of Practice meaning that the material is protected nonetheless. Under Chapter 7 of the Code, any individual selecting for examination material which relates to a sensitive profession, including journalists, must have regard to the potential infringement of the right to privacy and freedom of expression which could result from their examination. As set out in Chapters 8, 9 and 10, we review the justification records for examination of BPD material kept by each agency and we specifically consider the records kept in relation to any examination of material expected to relate to journalists.

Safeguards relating to sensitive professions

There are a range of different approaches taken within the various Codes of Practice (CoP) accompanying the sections within the Investigatory Powers Act in relation to sensitive professions. To some extent, these reflect whether the data has been acquired under an interception warrant, equipment interference warrant or retained as a bulk data set.

In our 2018 Annual Report, we highlighted that the Targeted Communications Data CoP contains detailed guidance for examination where the purpose is not to identify or confirm a journalistic source but where this is nonetheless likely. These protections are not mirrored in the Bulk Communications Data CoP. We believe that these crucial safeguards should be consistent, both in order to improve the level of understanding that members of these professions can have in relation to these protections, and to enable users to apply similar standards across the different powers they rely on. We have suggested to the Home Office that the CoP should be amended to ensure consistency.

Additional safeguards for health records

- 3.21 The intelligence agencies may apply for a specific Bulk Personal Data (BPD) warrant to retain and examine a dataset which includes health records. Any such applications are subject to an additional safeguard in that the case for retention and examination must be judged by the Secretary of State to be exceptional and compelling. We are unable to publish any details of whether, and to what extent, this power was used in 2019. However, we can confirm that we have not identified any issues of non-compliance or made any recommendations in relation to these safeguards.

4. Communications and engagement

Overview

- 4.1 Engagement with external organisations, both domestic and international, remains a priority for the Investigatory Powers Commissioner (IPC). Throughout 2019, we met with a range of non-governmental organisations (NGOs), academics, international oversight bodies and other independent bodies. Though there are inevitably limitations due to national security requirements, we feel there is real value in the continued cooperation with international partners; we have shared best practice in oversight regimes and learned from others' practices. This has included supporting gatherings of intelligence oversight bodies based overseas. The full schedule of the IPC's engagements is found at Annex E.
- 4.2 Our external communications increased towards the end of 2019 with regular announcements published on our website. These articles outlined the activity of the IPC, including contributions at conferences and events, and highlighted important areas of work for the organisation.
- 4.3 In the latter half of 2019, we appointed a Head of Communications and Engagement who has led on developing strategies for the organisation to improve transparency and increase engagement. This was a new role, which we hope will allow us to engage more widely and more consistently in the future to a range of partners and interested parties.

UK engagement

- 4.4 UK engagement has been a priority for both the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) during the period of transition to the Investigatory Powers Act (IPA). The primary focus through this period has been HMG and national-level bodies involved in reviewing and issuing guidance on the use of covert powers, the authorities using those powers and NGOs with a particular interest in the UK's activities in this area and the impact on human rights.
- 4.5 Reprieve, a legal charity which challenges the use of torture around the world, met with the IPC in 2019 and again later in the year with other senior staff at IPCO. Conversations centred on The Principles and the collection of data by IPCO. Reprieve's comments were welcomed in relation to IPCO's oversight of the Consolidated Guidance and details of their challenge are included in IPCO's 2018 report.¹⁰ The IPC hopes that conversations like this will continue to help increase the transparency around IPCO's work, debunking some of the myths around oversight.

¹⁰ Reprieve have raised concerns about the government's policies to prohibit involvement in torture and have questioned the balance of transparency and secrecy taken by parts of government, including the MOD, Intelligence Agencies and IPCO. Reprieve, "Review of UK Torture policy launched in U-turn from Theresa May" (2018), <https://reprieve.org.uk/update/review-of-uk-torture-policy-launched-in-u-turn-from-theresa-may/>

- 4.6 Last year, IPCO received a letter from Privacy International, an organisation which seeks to protect the right to privacy for all, regarding the use of social media intelligence by local authorities. In our response we outlined our approach to the oversight of local authorities, specifically how we encourage the development of policies and training of staff in this area. This correspondence has continued into 2020. The IPC would also like to expand his discussions with organisations like Privacy International to include the issues arising from OCDA's work, as he feels this would valuably inform the public debate about data and privacy. This is an area where we hoped to expand our engagement in 2020, but this has been impacted by the challenges posed by the COVID-19 pandemic.
- 4.7 In addition to the NGOs, we have had regular meetings with UK independent bodies including the Information Commissioner's Office (ICO) and the National Anti-Fraud Network (NAFN). Our Inspectors have explored options to collaborate with the ICO where responsibilities overlap. The two organisations published a joint letter on dual reporting, to prevent the duplication of work by public authorities and we are in ongoing discussions for the potential implementation of some joint inspections. With regards to NAFN, one of our Judicial Commissioners gave a talk on oversight at their annual conference and a number of Inspectors provided training and advice to NAFN's National Training and Best Practice working group.
- 4.8 In 2019, our Inspectors contributed to several national working groups (WG) to help inform security policy and procedures. These include the Home Office Covert Human Intelligence Source (CHIS) WG; the National Source WG;¹¹ the National Central Authorities Bureau (CAB) forum;¹² and the Internet Intelligence & Investigations group.¹³ Inspectors also liaised with the National Human Intelligence (HUMINT) Unit¹⁴ on Counter Terrorism policing policies and procedures. To help implement good practice in the use of investigatory powers by law enforcement agencies, we also offered input on training courses at the College of Policing and to larger public authorities such as the Metropolitan Police Service (MPS) and Greater Manchester Police (GMP). Judicial Commissioners Sir John Saunders and Lord Hughes were accompanied by several of our Inspectors to give a presentation and answer questions on our work at the 2019 National Undercover Conference.
- 4.9 We were also pleased to be invited to participate in a piece of research titled "Guardint; Oversight and Intelligence Networks: Who Guards the Guardians?" which is due to be published in 2020. Guardint is a collaborative project between King's College London and academics in France and Germany.¹⁵ Guardint aims to understand the role of oversight of intelligence agencies in democratic regimes, in the context of the expansion of transnational intelligence networks, and digital data collection and sharing. As part of this research project, three representatives from IPCO were interviewed on the work, set up and responsibilities of the organisation. We also provided information on the role of the Technology Advisory Panel, which gave an additional perspective on the oversight in place under the IPA.

11 The NSWG is a National Police Chief Council (NPCC) group dealing with CHIS matters with representatives from all main LEAs, a regional representative, MI5, MOD etc.

12 The NCAB is a similar NPCC forum with regional representatives for police forces and other agencies. The CAB (Covert Authorities Bureau) are the central units in an organisation that quality assure, oversee all RIPA issues and liaise with IPCO Inspectors. This group discusses emerging issues, IPCO inspection findings and guidance to ensure consistency amongst its members.

13 The Internet, Intelligence and Investigations Group is an NPCC group examining the development of online investigations (not including UC) to identify best practice, agree national policy, guidance and training.

14 The National HUMINT Unit is part of the CT Policing National Operations Centre. It co-ordinates and improves the HUMINT capability of counter terrorism policing and liaison and compatibility with MI5.

15 Guardint (2019), <https://guardint.org/>

- 4.10 A lot of work has been focussed on developing strong working relationships with stakeholders during OCDA's first year. Prior to each transition from the Regulation of Investigatory Powers Act 2000 (RIPA), to the IPA, this followed a structured path of engagement, and this has continued into business as usual. In addition to attendance at various communications data (CD) national forums and conferences, OCDA held a national stakeholder event in September 2019 to consolidate those relationships and reflect on performance in the first six months of live operations. Independence is key to OCDA's working model but building and maintaining professional working relationships with requesting authorities is necessary to make the authorisation process as efficient as possible and to make sure requestors have a strong understanding of the requirements imposed on them under the Act. OCDA will continue to prioritise engagement with requesting authorities and stakeholders involved in reviewing and issuing policy and guidance throughout 2020.

International engagement

- 4.11 As mentioned above our discussions with other international oversight bodies can be limited by matters such as our different remits and laws. However, these conversations are crucial to IPCO in helping us develop our ways of working and understanding where future challenges might arise.

Europe

- 4.12 We therefore attend a number of international conferences and engagements in Europe each year. For example, our Inspectors support the work of the European Union Agency for Fundamental Rights, specifically assisting the Head of Sector Information in the Society, Privacy and Data Protection Freedoms and Justice Department of Austria.
- 4.13 In 2019 we continued to support the Stiftung Neue Verantwortung (SNV), an independent think tank that aims to inform how German politics can shape technological change. The SNV hosts the European Intelligence Oversight Network (EION), a gathering of organisations that together explore intelligence oversight and build good practice. IPCO Inspectors attend EION meetings and, in 2019, they contributed to the EION research publication to explain the role and process of oversight in a transparent, understandable format. Specifically, Inspectors explained how they study data on their inspections, at times instructing agency staff to extract the data so that it can be examined in more detail by IPCO.

United Nations

- 4.14 Aside from a meeting for European oversight bodies in March 2019, these events predominantly took place in the latter half of the year. International partners came together for numerous conferences and working groups including the United Nations International Intelligence Oversight Forum (IIOF), which took place in London in October, and the European Intelligence Oversight Conference (EIOC), hosted in the Netherlands in December. With participants from governments, intelligence agencies, academics and NGOs, the IIOF focused on the future of intelligence oversight worldwide while taking account of fundamental human rights. In contrast, the EIOC is a forum solely for oversight bodies; the focus this year was on intensifying cooperation while keeping up with the advancement of technology.

Five Eyes

- 4.15 The annual Five Eyes International Oversight Review Council (FIORC) was hosted by IPCO in late 2019. We were delighted all five participating countries were represented (Australia, Canada, New Zealand, the UK and the USA). We agreed some key areas of work to focus on throughout the year to improve our understanding of the ways we work. Participants continue to meet virtually but the next council meeting in October 2020 has been cancelled due to the COVID-19 pandemic.



Sir Adrian Fulford with FIORC participants in October 2019

- 4.16 In December 2018, we responded to a request from the Royal Commission into the Management of Police Informants (RCMPI) which had been established in Victoria, Australia. The Commission wrote to the IPC for guidance on how CHIS activity is regulated and overseen in the UK. Lord Hughes provided our response, which included a teleconference with Australian officials where he gave an overview of the statutory basis in RIPA and explained how our Inspectors are able to oversee reliance on RIPA powers at inspection. The importance of safeguards around legally privileged material was a key focus of our response, as we believe this is a central pillar and a key strength of the UK's model. We expect to continue to work with RCMPI as they reach the stage of making recommendations for a future regime of management and governance for CHIS in Australia.
- 4.17 Australia's Independent National Security Legislation Monitor (INSLM),¹⁶ Dr James Renwick, visited London in November 2019 as part of his consultation for the Review of Australian Telecommunications legislation (TOLA Act 2018). Dr Renwick visited a number of countries, including the UK, to explore the different statutory models for the regulation of the use of modern digital investigatory powers. The Investigatory Powers Commissioner explained

16 Independent National Security Legislation Monitor (2019), <https://www.inslm.gov.au/>

how IPCO oversees the UK's use of investigatory powers, especially the function of Judicial Commissioners in authorising intrusive activity. The INSLM was also able to spend time with the Technology Advisory Panel (TAP) who advised on the impact of changing technology on oversight.

Other international groups

- 4.18 In March, representatives from IPCO and OCDA attended the International Communications Data and Digital Forensics conference (ICDDF).¹⁷ The ICDDF is an annual conference which recognises global excellence and collaboration in the investigation of digital and cyber-crime and intelligence in law enforcement and is attended by law enforcement agencies from around the world. At the conference, our Inspectors contributed to workshops and seminars with global partners, answering queries on investigatory powers procedures in the UK and IPCO's oversight.

17 International Communications Data and Digital Forensics (2019), <https://www.icddf.com/>

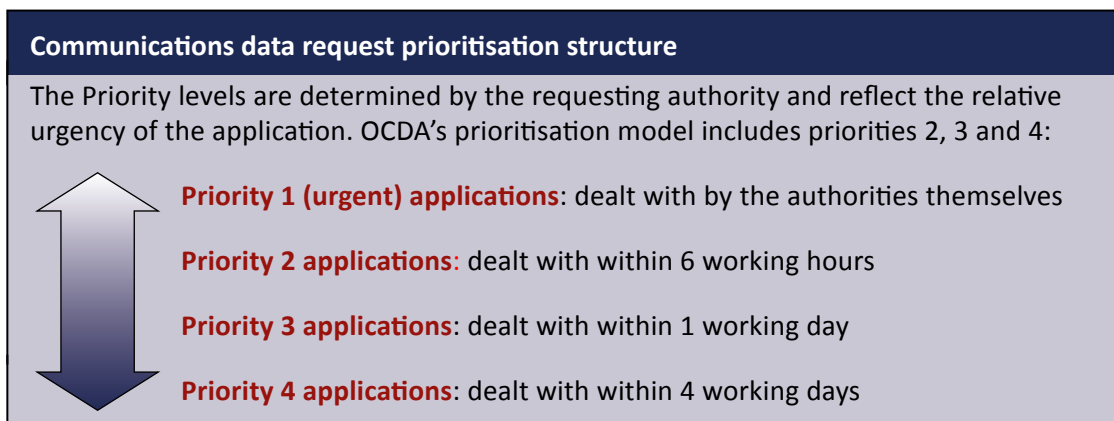
5. Office for Communications Data Authorisations (OCDA) processes and methodology

Overview

- 5.1 After two years of careful planning and a project delivery phase, the Office for Communications Data Authorisations (OCDA) became operational on 26 March 2019. OCDA operates out of two offices, in Manchester and Birmingham, from 7am to 10pm, seven days a week, with a total complement of just over 100 staff. OCDA is a separate organisation from IPCO but the Investigatory Powers Commissioner is responsible for the discharge of the functions of both offices.
- 5.2 Over the course of 2019, OCDA managed the transition of over 600 authorities from the Regulation of Investigatory Powers Act 2000 (RIPA) to the Investigatory Powers Act 2016 (IPA). This was a huge programme of organisational change which we ultimately found to be highly successful. The authorities we work with range from those submitting fewer than ten applications annually, through to the largest police forces, such as the Metropolitan Police Service (MPS), who submit over 26,500 annually. Annex D includes a full breakdown of communications data (CD) authorisations, which includes all applications that were approved by OCDA. This means that the challenges, both logistically and in terms of training and understanding, differ greatly across the requesting authorities.
- 5.3 We increased our workforce gradually during 2019, in line with the transition of authorities from RIPA to the IPA. Our staff joined from a variety of different backgrounds including law enforcement, other government departments, various private sector bodies as well as direct entry graduates. The body of Authorising Individuals at OCDA comprise a range of civil servants who have been trained to make and oversee decisions in relation to CD applications. The majority of OCDA's staff are Authorising Officers (AOs), who received a structured programme of training to become OCDA Authorising Individuals. The AOs are supervised by staff of a higher grade who also undertook the same training and are also OCDA Authorising Individuals.
- 5.4 IPCO's inspectorate supported the transition to independent authorisation by OCDA alongside colleagues from the Home Office. Inspectors were extensively engaged in the development of training material for the OCDA Authorising Individuals and delivered specialist training during their induction period. As OCDA became operational, IPCO sent Inspectors to OCDA's offices to assist with any issues arising and to provide technical advice. OCDA AOs also shadowed IPCO oversight inspections to gain a more thorough understanding of the end to end process.

Processes

- 5.5 We have a complex IT structure to meet the varied needs of the requesting agencies we work with. The majority of applications are submitted to us by individual authorities through their own workflow systems and received into our bespoke Case Management System (CMS). Applications are safeguarded within systems accredited to handle material classified as Official Sensitive, Secret, and Top Secret.
- 5.6 One of the greatest challenges when setting up OCDA was anticipating the number of applications that we would receive. This was essential to enable us effectively to prioritise and manage our workload so we could review and approve the greatest proportion of applications within routine processes. The Home Office analysed information from previous IPCO inspections of relevant authorities to predict the volumes that would be submitted to OCDA. Overall these estimates were helpful and we received 97% of anticipated applications at the end of the transition phase. Whilst numbers submitted by individual authorities varied from predictions at times, the overall number of applications we dealt with has been broadly as expected. One notable exception was the MPS, one of the largest requesting authorities; the MPS submitted 124% of anticipated applications and has exceeded the anticipated weekly number 90% of the time since transition. However, the work we had conducted to model and prepare processes meant that we were able to deal with this increase without compromising our service to the MPS or other applicants in any way.
- 5.7 Before starting live operations, we set out anticipated service level expectations, to guide requesting authorities, based on three categories of priority. We met these expectations throughout the year, except for four applications for which the returned decisions missed their deadlines. These delays occurred due to an oversight in regularly checking the relevant discrete IT system that was used to submit the four applications. We have made process alterations as a result and there have been no further incidents. We have been pleased to note that many authorities have commented that the speed of service provided by OCDA is superior to that previously in place when applications were authorised under RIPA.



- 5.8 When we receive an application, the Authorising Individual makes one of three decisions: to authorise, to reject or to return the application for rework. An application is only rejected when it is thought to be sufficiently flawed that it is considered unlawful; as a result, very few applications are rejected. Most applications that we refuse to authorise are sent back to the authority for reconsideration, referred to by OCDA as 'returned for rework'. This can be for several reasons, but frequently it is to seek clarification on the specific data requested or more detail relating to the justification or proportionality of the request.

We may also return an application for rework if it appears that there has been an error in drafting made by the applying authority, for example the authority may have selected a crime type that does not match the description of the offence. We have regular discussions with requesting authorities on those applications 'returned for rework' and this has been key to our stakeholder engagement.

- 5.9 Figures for the OCDA casework, including the number of applications received, authorised and withdrawn, are at Annex D.

6. Office for Communications Data Authorisations (OCDA) observations

Overview

- 6.1 During our first year, we believe that our processes and methodology have delivered efficiencies and standardised the process for considering, authorising and issuing communications data applications. We have also learnt from working with requesting authorities and have identified where differing processes and regional practices result in differences in approach which leave room for improvement. Elsewhere in this report, Inspectors of the Investigatory Powers Commissioner's Office (IPCO) have identified certain areas where OCDA has started to bring changes which we expect to continue throughout 2020.

Lessons learnt

- 6.2 In relation to law enforcement agencies (LEAs), IPCO raised concerns in 2018 that the crime being investigated was not well articulated on communications data (CD) applications. In particular, in applications we consider which can only be granted if the serious crime threshold is met, we expect there to be a clear explanation of how that threshold is met before the application will be approved (see paragraphs 12.46-12.52).
- 6.3 IPCO Inspectors have also advised public authorities to work closely with us to ensure that complex requests are clear and well documented. This is particularly the case for events data requests, which may be new to some authorities (see paragraphs 13.15, 14.5 and 14.15). We expect that ongoing engagement in this area will enable these authorities to submit adequate applications so that acquisition of the CD they need can be authorised.

Business improvement

- 6.4 The vital role OCDA plays for requesting authorities means that it has been essential to set up an organisation which is capable of reacting to changing circumstances. Business continuity has been a focus of our development, both in terms of our infrastructure and staffing model. We have proven our services are resilient during this year by dealing with an accommodation-related critical incident that closed our Birmingham office for several weeks; this was done with such efficiency that most stakeholders noticed only a minor degradation in service.
- 6.5 In the first months of operation, we identified areas where business improvement is necessary, including changes to our bespoke Case Management System and the way we handle applications from authorities who do not use an automatic workflow system. We intend to implement those changes during 2020, thus increasing our efficiency. We will also continue to consider other areas for business improvement.

7. Inspection methodology

Overview

- 7.1 We have continued to develop our model for oversight, which was outlined in full in our 2018 report. It is important that our inspection model is sufficiently flexible to enable us to respond to priority issues, such as the safeguards compliance mitigation work at MI5. We also seek to draw together a best-fit team to take an objective view of each of the authorities we oversee, delivering this through a joint inspection model for larger law enforcement authorities. This chapter summarises where we have changed our approach in 2019 and the chapters that follow detail the findings from those inspections.
- 7.2 We continue to work with three teams of Inspectors each managed by a Chief Inspector: one team covers targeted equipment interference (TEI), property interference, surveillance and covert human intelligence sources (CHIS), the second team examines the use of communications data (CD), and the third team inspects the intelligence agencies, Ministry of Defence and the other intercepting agencies.¹⁸ At the end of the year, we recruited a fourth Chief Inspector to lead the data assurance programme described below and we are in the process of recruiting specialist Inspectors to join this team.

18 Intelligence agencies: GCHQ, MI5 and SIS (MI6), the other Intercepting Agencies: HMRC, PSNI, Police Scotland, NCA, and MPS.

Definitions: investigatory powers

Targeted equipment interference:

This is the process by which an individual's electronic equipment may be interfered with to obtain information or communication. Activity could include remote access to a computer or covertly downloading mobile phone contents.

Property interference:

Examples of this is where there is a need to covertly interfere with physical property, such as goods, but it is also used for trespass to land in order to avoid civil or criminal liability: for example, trespassing to install a listening device in a person's house.

Surveillance:

Surveillance can be either directed or intrusive. Directed surveillance is covert but not carried out in residential premises or private vehicles, this could include the covert monitoring of a person/people of interest. Intrusive surveillance is carried out, for example, using eavesdropping devices in residential premises or in a private vehicle.

Covert human intelligence sources:

A Covert Human Intelligence Source (CHIS) is an individual who supports the functions of certain public authorities by providing intelligence covertly on a person of interest with whom they have a personal or other relationship. A CHIS under the age of 18 is referred to as a Juvenile CHIS.

Communications data:

Communications data is the who, where, when and how of a communication but not its content.

Judicial Commissioners

- 7.3 During 2019 Judicial Commissioners (JCs) have continued to play a part in some inspections, either as an observer or as part of the inspection team. Some of the notable inspections involving JCs have been Police Scotland, the National Crime Agency (NCA), Her Majesty's Revenue and Customs (HMRC), Greater Manchester Police, and Her Majesty's Prison and Probation Service (HMPPS). Where possible, we have aimed to align the inspections with a JC's particular portfolio interests, such as for Dame Linda Dobbs who has a special interest in custodial matters both here and overseas. Feedback from the JCs has shown that joining these inspections has enabled them to see beyond the documentary aspects of investigations in which they may have been asked to approve a warrant. This has enhanced their understanding and appreciation of the operational considerations and challenges faced by officers and helped them understand the evolution of the broader investigation, of which the covert activity might be just one aspect.

Example: Judicial Commissioners on inspection

Lord Bracadale joined the inspection of Police Scotland in 2019 and took charge of the examination of all relevant authorisations and warrants relating to two major investigations where a range of tactics had been used. This gave him a holistic view of the operation and enabled him to assess whether the use of the various powers had been necessary and proportionate. He was satisfied and was able to attend the final feedback session, together with a fellow Judicial Commissioner, and deliver his personal findings to the senior officers of the Force at the end of the inspection.

UK Intelligence Community (UKIC)

- 7.4 Inspections of UKIC are conducted throughout the year covering the range of powers we oversee. A full description of our methodology was contained within our 2018 report. In 2019, we additionally conducted a number of responsive compliance inspections at MI5 (see chapter 8) and have introduced cross-cutting safeguards inspections, which have enabled us to examine the implementation of key policies and practices across the range of powers. For example, we have looked at how legal professional privilege (LPP) policies are applied across an agency, as well as examining how well the relevant considerations are articulated in individual applications.
- 7.5 Continual dialogue with the agencies is a key part of our oversight because of the constantly developing nature of their work and change programmes in particular. During inspections, we often receive briefings on future planning such as IT improvement programmes; this gives us a valuable insight into the way each organisation is projecting compliance considerations for the coming decade. We have taken steps to formalise this process by introducing regular briefing days for our JCs and Inspectors, which we expect to give us a watching brief over relevant changes within each organisation. We will respond to these briefings by identifying areas for closer scrutiny at inspection and continue to apply a flexible working model throughout the team.

Oversight of bulk powers

- 7.6 Our oversight of bulk powers has evolved over the past year (see para 10.27). This reflected the European Court of Human Rights judgment in the *Big Brother Watch and others v UK* case, and the Intelligence and Security Committee's (ISC) *Privacy and Security Report* of March 2015. We reviewed our approach to inspecting bulk interception in 2019, considering the technically complex ways in which bulk interception is implemented and from 2020 our inspections will include a detailed examination of selectors and search criteria. This will supplement the oversight we have in place in relation to bulk personal datasets, bulk communications data and use of bulk warrants for interception, and equipment interference, which are inspected routinely across UKIC.
- 7.7 The Government Communications Headquarters (GCHQ) is the leading authority for bulk equipment interference. GCHQ transitioned its lawful authority for conducting equipment interference from the Regulation of Investigatory Powers Act 2000 (RIPA) warrants to warrants under the Investigatory Powers Act 2016 (IPA) during 2018. During 2019, we conducted our first full inspections of equipment interference conducted under the IPA. We conducted enhanced ex post facto oversight of the internal process used by GCHQ to approve operations conducted under these bulk equipment interference warrants. We selected cases in advance for scrutiny and where necessary, discussion with the teams

involved at the inspection. During our inspections we also had direct access (via a GCHQ operator) to the IT systems used to request and approve these activities, and we were able to select further cases for examination. We conducted our selection to ensure that we examined cases from a variety of business areas within GCHQ.

Law Enforcement Agencies

- 7.8 There have been no changes to our inspection methodology for law enforcement agencies (LEAs), other than the initiation of the data assurance programme. We have found that our methodology allows us to access both records and the personnel necessary to establish a clear picture of the compliance culture and processes at each force we visit.
- 7.9 We have continued to request details of use of powers ahead of each inspection and to require each force to demonstrate progress against previous recommendations.
- 7.10 All law enforcement agencies are inspected annually on their use of communications data (CD) and to inspect their use of property interference, surveillance, CHIS and equipment interference powers; some of these inspections are combined depending on how the force is structured. As noted in our 2018 report, we have conducted trials combining these inspections, or running them concurrently. This has the benefit of giving us a more comprehensive overview of operations across the force and, where the force governance is structured to cover both elements, this has strengthened the value and impact of our recommendations. In some cases, however, the distinct structure of the force means that this approach is not appropriate and so we have continued to conduct separate inspections. We have found that this does not impair the consistency and rigour of our inspections. From 2020, these inspections will also incorporate oversight of the use of targeted equipment interference (TEI). In many cases, TEI is conducted by regional specialists based in a regional organised crime unit (ROCU) and so we will be inspecting both activity at these hubs and the interplay with the forces they support. Annually, we also inspect all LEAs using interception powers.
- 7.11 A specific focus for 2019 has been the handling of intelligence, gathered as a result of the use of surveillance techniques or CHIS, to ensure that all relevant material is appropriately safeguarded and destroyed when retention is no longer justified. Decisions in this context continue to be complicated by the disclosure requirements of criminal proceedings, which meant that LEAs may be required to retain copies of intelligence for longer than otherwise would be operationally necessary. We have taken a more in-depth approach to testing whether staff properly understand the requirements of the law in this context in 2019 and will carry this on into 2020.
- 7.12 In relation to CD, our priority has been supporting the transition to the new model of approval via the Office for Communications Data Authorisations (OCDA). This has meant that we have focused on ensuring that new format applications are completed accurately and consistently across law enforcement.

Intercepting authorities

- 7.13 Since the introduction of the JC approval process to targeted interception warrants, our primary focus of inspections has been on those elements of the process that are not subject to the 'double-lock' under the IPA and so not subject to prior approval by IPCO. This has meant that the use of modifications has been a focus of our examinations in 2019. The effect of modification is to extend the scope of a warrant or to narrow it (by removing

selectors or subjects). It is important for IPCO to scrutinise decisions to modify after these are made, as well as at renewal, as a modification allows the authorities to intercept communications from both devices and subjects of interest who have not been addressed explicitly in the original warrant application. It is essential that the internal process is rigorous in considering and documenting the necessity and proportionality of intercepting additional communications methods, as well as persuasively setting out why it was not appropriate for the authority to seek separate warrants for each specific interception. To reflect this, our inspection methodology has focused on reviewing a higher proportion of modification documents and interviewing applicants.

Wider Public authorities

- 7.14 We inspect other public authorities, also referred to as 'wider public authorities' (WPAs), annually or bi-annually depending on the range of powers available, level of usage and compliance standards we have previously identified. A full list of these authorities is given at Annex A. In 2019, we inspected 26 WPAs.

Local authorities

- 7.15 Local authorities (councils) are inspected every three years, either by undertaking a physical visit which follows a similar format to other public authorities, or via a desktop assessment.¹⁹ Physical and desktop inspections may be undertaken on an alternate basis, so each council is visited at least once every six years. We also annually inspect local authorities via the National Anti-Fraud Network (NAFN), which processes all CD requests for local authorities.
- 7.16 Councils are typically low-volume users of their covert powers and so our inspections also investigate whether these powers are being used inadvertently by well-meaning but poorly trained or unaware staff members. To prevent this, we expect all councils to deliver training to key personnel at least once every three years and to have in place guidance that enables everyone to understand what investigative activity requires authorisations.
- 7.17 In 2019, we conducted 96 inspections of local authorities. Of those, we visited 50 and conducted 46 inspections remotely. We did not conduct any additional follow-up inspections.

Prisons

- 7.18 In our 2018 report, we noted that we were aiming to improve our inspections regime for prisons. We have worked closely with Her Majesty's Prison and Probation Service (HMPPS) and the Scottish Prisons Service (SPS) throughout the year to bring this to fruition. Details of our oversight and findings are detailed in chapter 15. Our oversight has now expanded and the first annual inspection of all 15 Scottish prisons was conducted between October 2019 and February 2020. During 2019 we inspected 114 prisons in England and Wales, 8 in Scotland, and 3 in Northern Ireland.

19 A desktop inspection is a paper-based review of policies, training materials and authorisation documentation, coupled with discussions by telephone or visual media with key officers of the public authority.

Data Assurance

- 7.19 Data assurance is a new programme of work that was launched in 2019 by the then Investigatory Powers Commissioner (IPC), Sir Adrian Fulford. This programme was initiated in response to the compliance issues identified at MI5, described elsewhere in this report (see chapter 8). This is an evolving area of work which will be resourced with two dedicated specialist Inspectors in 2020 and which has implications for all the authorities we oversee. We use the term “data assurance” to refer to the process of ascertaining that appropriate safeguards are in place for all data derived from the use of investigatory powers. Our objectives for this programme are:
- to inspect and investigate compliance with data safeguards to establish a high level of confidence that all data obtained under the powers overseen by the Investigatory Powers Commissioner's Office (IPCO) is retained lawfully;
 - to embed and encourage best practice for compliance at each authority we oversee; and
 - to assist the authorities we oversee to understand and investigate the compliance challenges arising from the use of bespoke, off-the-shelf and shared data handling programmes and technical storage environments.
- 7.20 Our methodology for this needs to be flexible and, given the scale of the activity we oversee, needs to take a risk-based approach. We therefore separated all the authorities into three groups. Group one is where we have focused the initial phase of our work and consists of LEAs and the intelligence agencies. The second group relates to wider public authorities grouped by available powers, with a third group for local authorities and those public authorities with similar powers. The first group are typically high-volume users of a wide range of powers, including those authorised under the IPA, so we therefore judge that it is appropriate that we investigate any potential non-compliance at these organisations as a priority. Conversely, the last group are typically low-volume users and in many cases are not currently obtaining any data under their powers. It is right therefore that we take a proportionate approach to our investigations.
- 7.21 As described at chapter 8, we have worked closely with MI5 to investigate compliance concerns in relation to a specific technical environment and have discussed the implications for the wider IT estate and future IT development. We had similar discussions over the summer with GCHQ and the Secret Intelligence Service (SIS) and have initiated safeguards inspections which will be conducted from 2020.
- 7.22 For group one, in the autumn, we wrote to all LEAs asking them to complete a self-assessment of their data holdings.
- 7.23 By the end of 2019 we had conducted an initial analysis of these returns and had identified key vulnerabilities which required further investigation (these are set out in chapter 12). We had originally intended to visit all forces in the UK throughout 2020 and had hoped to present findings in our 2020 report. However, this work has been delayed by the pandemic and, although we will have visited all forces where key vulnerabilities will have been identified by November 2020, there will be some forces where a visit will not have been possible. Therefore, we now expect this work to continue into 2021 and we will provide an update on this in next year's report.
- 7.24 For group two of the programme we have requested that public authorities should complete a self-assessment. Analysis of these returns is ongoing.

- 7.25 In relation to the third group, all local authorities have received a letter reminding them of their obligations to safeguard data obtained under their powers. At all future inspections we will investigate whether they are holding data properly and will discuss these obligations with them.

Data compliance self-assessment

The self-assessment request asked the following questions in relation to each power used by the force:

- Does your authority collect data under investigatory powers?
- Does your authority retain data collected under investigatory powers?
- Does your authority retain data collected under investigatory powers on bespoke data handling or IT systems? If so, what are they?
- Does your authority use systems outside of the primary workflow/data handling system to back up or analyse the data? If so, what are they?
- Does your authority retain data collected under investigatory powers which is then processed on a system outside of the organisation's IT estate, such as a server operated by a commercial organisation (possibly as part of a service agreement (i.e. cloud computing))?
- Are there access, retention and destruction safeguards in place across your data handling and IT infrastructure? If so, what are they?
- Who is responsible for ensuring that these safeguards are fully enacted?
- Are you aware of any areas of your data handling or IT infrastructure which do not apply access, retention and destruction safeguards?
- Does your authority adhere to any additional policies in relation to access, retention and destruction of data obtained under investigatory powers?

8. MI5

Overview

- 8.1 This chapter, and those that follow, summarise the key findings from inspections which were conducted in 2019 by the Investigatory Powers Commissioner's Office (IPCO). The methodology for our inspections is summarised at chapter 7 above.
- 8.2 We conducted regular inspections of MI5 throughout 2019, including four extraordinary inspections in response to compliance risks identified in February. A substantial proportion of MI5's use of investigatory powers is conducted using powers that are subject to the double lock. This gives us oversight of the range of live operations as well as post facto oversight through our inspections. During our inspections, we have interviewed operational staff, legal and policy representatives and senior management at MI5 to give us insight into their policies, practices and culture of compliance.

Findings

- 8.3 In general, we found a good level of compliance across all powers, noting that the casework we saw was completed to a high standard and staff demonstrated a commitment to applying powers in a measured and lawful way. As in previous years, we have seen MI5 working to review and improve internal policies and processes across their business and we are pleased to be sighted on future planning and strategies. It is worth noting that we have been involved in discussions and planning in relation to the recommendations made by Sir Martin Donnelly's Compliance Improvement Review. We expect this work to result in refreshed processes and structures within the organisation which will enhance compliance and operational agility.
- 8.4 The compliance improvement programme (see paragraphs 8.56 – 8.58) impacted upon our oversight at MI5 throughout 2019, not least because of the substantial resources placed on this work by MI5. We were pleased by the clear and consistent insight MI5 provided into this programme and believe that this will have a significant positive impact on MI5's compliance culture for the coming decade.

Covert human intelligence sources (CHIS)

- 8.5 MI5 authorise all their CHIS operations in the UK, and the majority of those conducted overseas, under the Regulation of Investigatory Powers Act 2000 (RIPA). Some overseas operations do not require RIPA authorisation but are nevertheless subject to detailed operational assessments. We review this documentation as part of our CHIS inspections.
- 8.6 Overall, we have concluded that MI5 continue to manage CHIS activity in a highly professional manner and are mindful of the ethical implications of this work. We found the quality of consideration by handlers (those actually meeting and tasking the CHIS),

Authorising Officers (AOs), and legal and security advisors to be especially high when dealing with the most challenging CHIS cases.

- 8.7 MI5 have responded positively to recommendations made at previous inspections and we observed a marked improvement in the way that CHIS records are now maintained. However, there is still room for greater consistency in relation to the carrying out and recording of reviews and the setting out of considerations in relation to necessity, proportionality and collateral intrusion by AOs.

Definition: collateral intrusion

Collateral intrusion is the interference with the privacy of individuals who are neither the targets of the operation, nor of intelligence interest, for example background conversation of passers-by recorded with the speech of the target. We expect public authorities to proactively assess the possible extent of collateral intrusion in any proposed activity and, where possible, take reasonable steps to mitigate this.

- 8.8 MI5 have implemented changes to their processes following our detailed examination of their online CHIS activity in 2018. We expect that full implementation of these changes will ensure that each officer engaged in such activities is separately authorised under RIPA, rather than one online persona or profile which may be being used by several individuals. This change will also include a clear description of the proposed use and conduct in each case. Likewise, we recommended that a separate risk assessment must be completed for each officer addressing the risks specific to that individual. We will continue to closely monitor the implementation of these recommendations during 2020.
- 8.9 As in all areas, we carefully balance the requirement to properly test compliance against the need for access to records and operational personnel and the sensitivity of the information we are reviewing. We do not believe it would be proportionate to review all CHIS paperwork, which would inform our Inspectors of the true identities of all current and former agents. We are also content that there is no requirement to review all records and internal notes made by those involved in tasking and safeguarding CHIS given the high level of compliance and professionalism that we see in these departments. However, we are working with the agencies to review the type of access that we have to CHIS records. The UK Intelligence Community (UKIC) uses a variety of formats and systems to handle and safeguard CHIS material, which can make it more difficult to conduct a comprehensive review of a single casefile, if required. We have therefore asked the agencies to look again at the most effective method of presenting all relevant documents at inspection.

CHIS Participation in Criminality (PIC)

- 8.10 MI5 has an internal policy governing PIC by CHIS which relates to both recruited agents and MI5 officers operating under cover in both the real world and online. The Investigatory Powers Commissioner (IPC) is required by the Prime Minister to oversee MI5 compliance with this policy by virtue of a direction that was first made public in 2018. An earlier iteration of this requirement has become known as "The Third Direction" and was the subject of litigation in the Investigatory Powers Tribunal (IPT) in 2019. The IPT gave its judgment in late December 2019 and found MI5's policy to be lawful, although permission to appeal this decision has been granted.
- 8.11 As in recent years, we examined a high proportion of PIC cases to ensure that MI5 was acting in line with its PIC policies. Inspectors have observed the comprehensive

consideration given to such activity by case officers, managers, operational security advisors and legal advisors before any such activity is approved. We are content that MI5 policy was correctly followed in every case that we inspected.

- 8.12 MI5's policy requires officers clearly to set out and record parameters for CHIS behaviours which might involve criminal activity. It remains the case, however, that authorising officers do not always lay out clear parameters under which the CHIS may operate and we have recommended that there should be greater consistency in this area. We have also noted that PIC authorisation documents are not subject to review, update or cancellation, as would be the case for the RIPA authorisations in place for the CHIS they relate to. We have observed that this would be a useful discipline, although we understand that this is not a requirement under the policy.
- 8.13 In respect of PIC conducted by CHIS online, MI5 has sought to authorise the online persona rather than the individual CHIS that would be undertaking the activity. We believe that this leaves room for some confusion and inconsistency in approach. We anticipate that a change in line with the general authorisation of individual CHIS rather than personas would be beneficial.

Juvenile CHIS

- 8.14 The use of underage individuals as agents is a sensitive area of work and we are unable to disclose whether any of the intelligence agencies or Ministry of Defence have recruited individuals under the age of 18. Irrespective of whether they had any active casework, we would expect each agency to maintain appropriate policies and practices that would ensure that any such agents were properly handled and protected. We are satisfied that MI5 has policies in place regarding the recruitment and running of juvenile CHIS.

Directed Surveillance

- 8.15 We raised a concern with MI5 in 2018 in relation to their review processes for directed surveillance authorisations (DSAs). We found that MI5 did not have an adequate review process in place for this commonly used power, which meant that authorising officers were not properly setting out their considerations of necessity, proportionality and collateral intrusion for continued operations during the period for which a DSA was authorised. We advised MI5 that their informal, often verbal, review processes fell short of the requirements of the Code of Practice (CoP). We also highlighted a lack of specificity on documentation for authorisations that covered a range of powers: MI5's renewal casework commonly did not justify the continued use of the full range of techniques and cancellation records often lacked detail regarding the activity undertaken and value to the investigation and operation.

Definition: directed surveillance

Directed surveillance is covert but not carried out in residential premises or private vehicles, this could include the covert monitoring of a person/people of interest.

- 8.16 We have challenged MI5's policy of noting authorising officer comments for surveillance only in exceptional cases. In the vast majority of cases, this means that there is no record of any consideration by the authorising officer. We recommended that it would be more appropriate for a routine notation of considerations to be made in each case. We believe

that this would give authorising officers greater ownership of the process and would increase our level of confidence in this process.

- 8.17 In response to a number of recommendations relating to DSAs, MI5 implemented an action plan. However, we were disappointed that this had failed to deliver the necessary improvements by our second inspection in November. MI5 have formulated a new action plan targeted at authorising officers and our first inspection in 2020 will focus on monitoring the progress of remedial action against these recommendations.
- 8.18 In general, however, the standard of MI5's surveillance documentation and supporting policies is good and we underline that we reviewed a small proportion of their casework. We focused on thematic authorisations and were clear in each case that this was the appropriate means of authorising the proposed actions. In some cases, we noted that the scale of the planned operation could be more clearly articulated. We expect that the reliance on thematic authorisations, to which individual targets may be added and removed, will be addressed as part of the above programme of work and expect to see recording of more consistent reviews of individuals named on any active authorisation.
- 8.19 We have encouraged MI5 proactively to brief us on new techniques and tools, which gives us the opportunity to discuss any potential legal issues at the earliest opportunity. MI5 drew to our attention two cases which related to an experimental surveillance capability. We noted that the records relating to these cases were of a high standard and demonstrated that MI5 had engaged legal and ethical experts in the planning of novel operations.

Property Interference

- 8.20 MI5's work under property warrants relies on tried and tested techniques and our oversight in 2019 did not identify any substantial issues. As with the other agencies, a proportion of the activity previously conducted solely under Intelligence Services Act (ISA) section 5 is now conducted under the Investigatory Powers Act 2016 (IPA), either because it is equipment interference, or as part of a combined equipment interference warrant. This means that our Judicial Commissioners (JCs) approve warrants covering a substantial proportion of MI5's operations relating to property interference and have found that the casework for the proposed operations continues to be of a high standard.
- 8.21 Once it is considered no longer to be necessary and proportionate to continue to collect eavesdropping product from devices installed within a target property, MI5 will stop actively monitoring the device and will plan to remove the device from the property. This can be a challenging activity and in some cases it is necessary to declare the device 'irretrievable'. In all cases, the device will eventually become inactive, incapable of being monitored despite its ongoing presence in the property because of, for example, a dead battery. The Commissioner has noted that the preference should always be to extract that equipment at the earliest opportunity with minimal intrusion into the privacy of the occupant(s). MI5 is continuing to review the way in which devices are retrieved to maximise the opportunity to do so but are looking to ensure this is carefully balanced against intrusion considerations.

Targeted Interception (TI) and Equipment Interference (EI)

- 8.22 MI5 continues to make extensive use of combined warrants under Schedule 8 to the IPA. During 2019 we conducted a single combined inspection looking at Targeted Interception

and Targeted Equipment Interference authorised under the IPA. MI5 does not undertake interception or equipment interference activity under bulk warrants.

- 8.23 Overall, we are satisfied that MI5 has achieved a high level of compliance with the IPA in respect to Targeted Interception and Targeted Equipment Interference. The warrants were necessary for one or more of the purposes set out in the Act and were proportionate to what they sought to achieve.

Rejected warrants

- 8.24 A JC rejected one application for the renewal of a combined Targeted Interception and Targeted Equipment Interference warrant from MI5. The circumstances of the case were that data could not be obtained at the time of the renewal and had not been obtained in the previous period but MI5 assessed that their officers might be required urgently to conduct actions under the warrant if the subject of the warrant was released from custody. The JC considered that the renewal was driven by considerations of administrative convenience and was neither necessary nor proportionate. The JC considered that, if the subject was released, MI5's operational team and the Home Office warrantry team might need quickly to apply to put monitoring techniques in place, but that this should not be prioritised over the subject's rights to privacy.

Additional reviews imposed by the Secretary of State

- 8.25 Under the IPA, interception and EI activity is authorised by the Secretary of State and approved by a JC through the double lock process. In some cases, for instance where there are concerns about the potential level of collateral intrusion, the Secretary of State may authorise a warrant but seek an early review of necessity and proportionality by the requesting agency. MI5 typically informs the Secretary of State of the result of these reviews in a letter of clarification. Overall, we discovered that in the vast majority of cases a letter of clarification was completed as requested and that the reviews satisfied the areas of potential concern. In the small number of cases where this had not happened, there was a satisfactory explanation for this. We found the reviews to be informative, accurate and relevant to the requests.

Confidential material

- 8.26 We selected and reviewed a number of warrants under which confidential material had been obtained. We were satisfied that MI5 handled any such confidential material carefully and in accordance with the legislation. During 2019, MI5 changed their legal professional privilege (LPP) policy to align it with the requirements of the IPA and to mirror the arrangements of the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ), which we believe is an appropriate approach. MI5 had previously applied the test of an "exceptional and compelling" case to justify the retention of any LPP material obtained under a warrant. This is a more stringent test than that set out in the IPA, which requires a balance of public interest test to be applied. MI5's policy was developed before the IPA came into force, hence the inclusion of a different and higher test than the one the IPA actually requires. MI5 has now amended the policy to refer to the balance of public interest test but we do not expect this to make a significant difference to how they are retaining LPP in practice.

Thematic warrants

- 8.27 We examined a number of thematic targeted interception warrants where applications had been made for both major and minor modifications to add new subjects and factors. All were properly authorised and consistently completed to a very high standard, with a clear rationale for adding or removing factors. Each modification clearly demonstrated the necessity and proportionality case as well as linking the new factor or individual to the subject and purpose of the warrant. If there was any change in potential collateral intrusion as a result of a new factor being added this was clearly addressed. There was good evidence that factors were being deleted promptly when no longer required, demonstrating good housekeeping.

Definition: factors

A factor is a description used to identify the communications to be intercepted under a warrant such as an address, a number or piece of apparatus. This could include a postal or email address, a telephone number or a device's Media Access Control (MAC) address.

General descriptors

- 8.28 The IPA allows for the use of "general descriptors" in circumstances where it is not practical to name or describe all of the subjects at the point the warrant is issued. The Interception and EI Codes of Practice (CoP) advise that the practicability of providing individual names or descriptions will need to be assessed on a case by case basis and will depend, for example, upon the existing intelligence picture, the scale and pace of the operation, the nature of the communications to be intercepted and/or from where secondary data is to be obtained, the nature of the factors (or equipment to be interfered with) and the time constraints of the particular operation.
- 8.29 We reviewed a number of warrants which included general descriptors. Overall, MI5 officers provided clear justification for why they needed this type of warrant and the flexibility of adding new subjects under the general descriptor. In some earlier applications we noted a degree of confusion as to what was necessary to justify the use of a general descriptor with some applications focussing on why all of the potential future subjects of the warrant were not identified yet, or the fact that, at the point MI5 required coverage of new subjects, they may not be fully identified. This is not relevant to the question MI5 is required to address. Rather, the use of a general descriptor should be justified in the application taking account of both the IPA's other requirements on necessity and proportionality and the guidance in the CoP that the overall intrusion to be authorised must be clear to the issuing authority at the time the warrant is issued. We saw no such confusion in more recent applications.

Testing and training warrants

- 8.30 Section 17(2)(c) of the IPA provides for agencies to obtain interception warrants for testing and training purposes, whilst sections 101(1)(g) and (h) provides for warrants for the testing, maintenance and development of equipment interference capabilities and training in the use of such capabilities. In 2019 MI5 applied for small number of training and testing warrants under the IPA. All but one of these superseded pre-existing warrants (including one which was put in place to supersede several earlier authorisations including non-IPA warrants).

- 8.31 We discussed this with MI5 at our October inspection and, as a result, we will be seeking further information in 2020 on a number of points. These questions are mainly in relation to safeguards relating to the users of the testing devices and the storage and retention of any material.

Bulk communications data (BCD)

- 8.32 MI5 holds a bulk acquisition warrant relating to several UK telecommunication operators.
- 8.33 Until 8 October 2018, the MI5 process for accessing BCD, which was acquired and retained by the agency via directions under section 94 of the Telecommunication Act 1984, substantially mirrored that set out in Chapter 2 Part 1 RIPA and the Codes for the Acquisition and Disclosure of Communications Data. That process required the investigator or analyst to set out in an application why it was necessary and proportionate to access the data. A designated person of appropriate seniority in the organisation then considered whether to give authority for that access.
- 8.34 This process changed substantially once bulk acquisition warrants under the IPA were introduced in October 2018. In accordance with the requirements in the IPA, the investigator or analyst is now required to create a record prior to selecting the data for examination, recording why the proposed examination is necessary and proportionate for a specified operational purpose.
- 8.35 During inspections, we are given access to the system used by MI5's investigators and analysts to record why the examination of specific data is both necessary and proportionate. This ensures we can examine the activities of specific members of staff who are authorised to undertake the examination of BCD. During inspection we undertake random sampling and run query-based searches on the system.
- 8.36 We scrutinise the majority of records that indicate the communications data (CD) sought relates to a person who may work in an occupation regarded as a sensitive profession. For example, we search for records which included the words 'medical practitioner' or 'journalist'. We examine the analysts' and investigators' necessity and proportionality considerations, examine particular operations and identify requests for more intrusive data sets including multiple communication addresses or those requiring data over longer time periods. We also interview members of staff to probe their considerations around these complex operations or sensitive requests.
- 8.37 Overall, we concluded that MI5's recorded justifications to undertake the examination of BCD were of a good standard and satisfied the principles of necessity and proportionality. The operational teams were interviewed and demonstrated the value of BCD to recent operations.

Bulk personal datasets (BPD)

- 8.38 In MI5, a service-wide gate-keeping panel, called the Bulk Oversight Panel (BOP) acts as a single point of contact for staff needing to obtain, retain and use bulk personal datasets. Each dataset acquired and held by the agency will have an allocated data owner who is responsible for considering the ongoing necessity of holding that data and assessing the value of its use. Data owners apply to the panel with requests to acquire, retain, renew, cancel or delete BPD and BPD warrants. The panel consists of senior managers and meets

monthly. Minutes, decisions and communications regarding the panel are available for scrutiny during inspections.

- 8.39 We have observed the positive development of the BOP and note its impact in managing internal compliance. We continue to seek greater clarity regarding the process MI5 uses to carry out initial examinations of new data sets to better understand decisions to classify a dataset as BPD or, for example, as targeted data. We were concerned by one unresolved action on the BOP minutes around resolving discrepancies between allocations of BPD between MI5 and SIS. It is possible, because of the different uses of the data and the different cuts of data being held, that both agencies could hold the same dataset, or versions of it, and that it could lawfully be categorised as bulk by one and targeted data by the other. There is a risk that, if one of the agencies has incorrectly categorised the data holding as targeted then that data would be held without appropriate warrant and might not be subject to appropriate safeguards. We suggested that this question should be resolved as a priority.
- 8.40 MI5 also enhanced their internal reviews of the justification used by staff to examine or query BPD. In compliance with the CoP, each agency requires staff to justify why they need to run a search on BPD in advance. For MI5 officers, this enables task-based searching, which allows more than one search to be conducted on a theme. For example, if an investigator is working to identify a specific individual or event they may conduct more than one search of the BPDs available to them. The system will track those searches, and the central audit team will review whether searches are appropriately justified. We have advised that as the audit team grows in sophistication then they should focus on assurance around this task-based process.
- 8.41 We have been pleased to note that the continuous review process required by the IPA is now in place in relation to justification records and we have made a number of recommendations to enhance and improve this process. This will be an area of greater focus during next year's inspection, when we intend to conduct more granular audit of search activities conducted under specific justification records. In preparation for that, we will also be looking more deeply into the safeguards in place for the systems holding BPD. We have requested further details of staff access and the levels of systems' audit.

Operational purposes

- 8.42 We continue to be satisfied that the use of operational purposes in relation to the examination of BPD by MI5 is appropriate. The records kept in this regard are clear and demonstrate appropriate use of this data.
- 8.43 As noted in 2018, we have seen evidence that the majority of datasets held by MI5 need to be made available to investigators and analysts working across a range of business areas. Specific, trained staff within certain areas of MI5 require this access to complete a variety of operational tasks and we are satisfied that MI5's approach is compliant with the CoP and legislation. We did not expect to see, and did not see, any requests to modify the operational purposes on a BPD warrant in 2019.

Non-compliance investigation and safeguards

- 8.44 As noted in our 2018 report, we were informed by MI5 in February 2019 of serious compliance risks associated with certain technology environments in use by MI5 (here after referred to as "TE1" and "TE2"). The detailed investigation launched by the then

IPC, Sir Adrian Fulford, in response has now concluded; this section of our report sets out the sequence of events and our key findings. In the future, safeguards will form a key part of our oversight at MI5 as well as the other authorities we oversee (see chapter 7). Throughout 2020 we will work with MI5 to build our level of confidence in the compliance of their IT estate with their legal obligations. We are confident that MI5's internal review of safeguards, initiated following the realisation of the severity of this issue, will identify any substantial vulnerabilities in their data handling model.

TE1: Initial investigation

- 8.45 MI5 first briefed the IPC on compliance risks associated with TE1 on 27 February 2019. MI5 then formally reported these risks in a letter to the IPC on 11 March. The key compliance risks highlighted in MI5's briefing were that, within TE1, MI5 had less assurance than they would wish regarding where data was stored in the environment; who had access to it; the extent to which it was being copied or shared; and the deletion processes which applied to it.
- 8.46 We conducted our first inspection of TE1 on 18-22 March, with the assistance of the Technology Advisory Panel (TAP). Our key conclusions related to:
- access controls;
 - copying of data;
 - review, retention and deletion of data;
 - legally privileged material: MI5 had a manual process in place for deleting legally privileged material from its systems if required to do so; and
 - institutional knowledge: having reviewed a number of MI5 internal documents we concluded that, by January 2018 if not earlier, MI5 had a clear view of some of the compliance risks around TE1, to the extent that it should have carefully considered the legality of continuing to store and exploit operational data in TE1. The risks were also sufficiently clear that they should have been communicated to the IPC at that time.
- 8.47 In response to our findings, MI5 initiated a series of mitigations which sought to secure compliance with the requirements of the IPA regarding the handling of warranted data. The IPC then made a determination on 5 April on the extent to which MI5 could be said to comply with the relevant IPA safeguards. He concluded that, subject to certain critical caveats, he was satisfied that MI5 had the capability henceforth to handle warranted data within TE1 in a way which was compliant with the IPA. He emphasised that *"all the relevant activities must be susceptible to inspection and audit – in other words, MI5 and IPCO must be able to check in sufficient detail that there has been compliance with the legislation"*.
- 8.48 In coming to this decision, the IPC also noted:

This is a serious and inherently fragile situation. The future will entirely depend on compliance by MI5 with the legislation and the adequacy of the internal and external inspection regimes. IPCO will need to be reassured on a continuing basis that new warranted material is being handled lawfully. In the absence of this reassurance, it is likely that future warrant applications for data held in [TE1] will not be approved by the Judicial Commissioners, and I will expect that the proposed mitigations are progressed at pace. The weaknesses outlined above are of sufficient magnitude to mean that the immediate mitigatory steps, which will be sufficient for the short term, cannot be expected to provide a long term solution, and the proposals made by MI5...must be

implemented in their entirety in the shortest reasonable timeframe...the historical lack of compliance with the law is of such gravity that IPCO will need to be satisfied to a greater degree than usual that it is "fit for purpose".

TE1: follow-up inspections

- 8.49 In the light of the IPC's comments above, we conducted further inspections of TE1 in April, June and September 2019. Each of these inspections examined the progress made by MI5 in delivering its remediation measures to reduce the level of compliance risk associated with TE1. In total, we spent 48 days at MI5 investigating the issues in depth and the IPC and his Deputy were closely involved throughout.
- 8.50 Throughout this period, MI5 devoted very substantial resources both to the programme of work to fix the compliance problems in TE1 and to facilitate our inspections. MI5's candid and open approach throughout all four inspections gave us a good degree of confidence in the conclusions reached at the end of our investigation, which are set out below.
- 8.51 Having regard to the relevant requirements of the IPA, in particular the "minimisation requirements" and the safeguards for legally privileged material, we are now satisfied that MI5's remediation work in TE1 has secured compliance with the required standards. Where possible, technical "fixes" have been implemented to enforce compliance requirements. MI5 should continue to look for, and implement, technical improvements wherever this is reasonably practicable.
- 8.52 Where technical changes to TE1 have not been possible, MI5 has introduced a range of manual processes to ensure its staff use TE1 in a compliant way. The most important aspects of this manual approach are a set of centrally agreed business processes governing how warranted data must be handled in TE1, backed up by regular assurance reviews conducted within individual business areas. It is critical that MI5 continues to maintain these new processes and to provide sufficient resources for them to function effectively. If MI5 identifies an increase in non-compliant behaviours in TE1, we would expect this to be brought to IPCO's attention as soon as possible.

TE1: MI5's institutional knowledge and disclosures to IPCO

- 8.53 In his determination of 3 April, the IPC commented as follows:

It is clear that for warranted material in [TE1] there has been an unquantifiable but serious failure to handle warranted data in compliance with the IPA for a considerable period of time, and probably since IPCO first became operational. Assurances that have been made to the Secretary of State and the Judicial Commissioners of such compliance were, in hindsight, wrong and should never have been made. Warrants have been granted and judicially approved on an incomplete understanding of the true factual position. Indeed, I am concerned that on this important subject we were incompletely briefed during the Commissioners' induction programme...To date, therefore, MI5's retention of the warranted material in [TE1] cannot be shown to have been held lawfully and the failure to report these matters timeously to IPCO is a matter of grave concern.

- 8.54 As mentioned earlier, this issue is now the subject of litigation before the Investigatory Powers Tribunal. Given the detailed information we have collated on TE1 since this was first brought to our attention, we are prepared to provide any assistance required of us by the Investigatory Powers Tribunal or other body in the future.

TE2: Errors reported to IPCO

- 8.55 In the course of its internal investigation into the compliance problems with TE1, MI5 also identified a number of relevant errors associated with the handling of warranted data within a second technology environment, TE2. These all arose because of a failure consistently to apply the correct retention period to some of the data held in particular parts of TE2, such that the data was being retained by MI5 longer than was necessary in pursuit of its statutory functions. Having reviewed these errors with MI5, we are satisfied that MI5 is taking all reasonable steps to delete the data concerned and ensure that similar errors do not arise in future. Whilst these errors were reported to IPCO in the course of MI5's investigation into TE1, we are confident that TE2 does not present compliance risks of a similar scale to those presented by TE1 in the early part of 2019.

Compliance Improvement Review

- 8.56 In response to the compliance problems identified in TE1, the then Home Secretary commissioned Sir Martin Donnelly in May 2019 to lead an independent review to identify lessons which could be learned for the future. Known as the Compliance Improvement Review (CIR), Sir Martin's report was published on 15 July 2019. A summary of the report's conclusions and recommendations is available on gov.uk.²⁰

- 8.57 One of the CIR's recommendations required IPCO's involvement:

There should be an urgent programme to provide staff, including contractors, with tailored best practice training on MI5's statutory obligations in respect of handling warranted data. This should draw on experience elsewhere in UKIC, with input from IPCO's inspectorate on the level of detail required.

- 8.58 In response, MI5 has shared the content of its new and improved training programme with us in draft, and we are in dialogue with them about their future training plans. The material we have seen to date is sufficiently detailed to give staff a comprehensive understanding of the compliance and legal requirements which are relevant to their respective roles.

Consolidated Guidance

- 8.59 MI5 has a clear and comprehensive internal policy to ensure its officers comply with the Consolidated Guidance. This includes a requirement that an internal form be completed any time MI5 is involved in activity that engages the Consolidated Guidance, even if the proposed course of action is low risk.
- 8.60 Where MI5 teams are passing intelligence to higher risk foreign liaison partners, they are almost always doing so in reliance on SIS ministerial submissions which are separately inspected by IPCO. As such, the decisions MI5 makes internally tend to be at the lower end of the risk spectrum. We have recommended to MI5 that, where appropriate, they might consider making greater use of so-called "thematic" internal forms. These set out the evidence behind MI5's judgement that all intelligence sharing with a particular partner is low risk, and permit MI5 to share intelligence with that partner in cases that engage the Consolidated Guidance for the next six months unless there are reasons to believe the risks have changed.

20 Sir Martin Donnelly, "Compliance Improvement Review" (15 July 2019), www.gov.uk/government/publications/compliance-improvement-review

- 8.61 In our 2018 report, we noted that MI5 was attaching a range of caveats to intelligence passed to foreign liaison partners and sometimes used the wrong caveat. All of the caveats we saw on our 2019 inspection had been used appropriately.
- 8.62 We identified one instance where MI5 failed promptly to investigate allegations of mistreatment which appeared in an intelligence report. Owing to competing priorities, the report's content was not reviewed in detail by the relevant team for several weeks; once the allegation had been spotted, it was then referred to the relevant specialist team in UKIC for assessment. However, UKIC were having regular discussions with partners to monitor the general compliance situation in the country in question during this time. We were satisfied with how the issue was handled from the point of it being referred to the specialist team but would not expect delays of this kind to occur in the future. Following investigation, it was determined the allegation was not credible.

9. Secret Intelligence Service (SIS)

Overview

- 9.1 We conducted regular inspections of the Secret Intelligence Service (SIS) in 2019. The majority of our investigations related to their work overseas, which is SIS's primary focus. The Deputy Investigatory Powers Commissioner (IPC) oversaw our work with SIS. As in previous years, we conducted inspections at three overseas stations, speaking to the range of operational staff working at each station about their work under section 7 of the Intelligence Services Act (ISA) and more broadly. During our London inspections, we speak to officers based overseas, as well as legal and operational staff working in the UK. This provides an opportunity for us to consider the working culture at SIS and the level of understanding of the legislative framework, both for officers working overseas and in the UK.
- 9.2 In October 2019, the IPC wrote to the Prime Minister about oversight of SIS's agent running activities overseas. This activity has a statutory basis under section 1 of the Intelligence Services Act 1994 (ISA). SIS agent running overseas is subject to oversight by the Investigatory Powers Commissioner's Office (IPCO) only in so far as it involves approvals under section 7 of the ISA. All other overseas agent running is not, and has never been, subject to oversight by IPCO or its predecessors. Further, the obligations under Part 2 of Regulation of Investigatory Powers Act 2000 (RIPA) do not apply to overseas agent running.
- 9.3 In his letter to the Prime Minister, the IPC acknowledged that the Government may have taken a policy decision that the running of agents overseas requires less detailed and intrusive oversight than those run in the UK. However, the IPC recommended that the Government ought carefully to consider whether this is still the right policy position. We expect to receive a response to the IPC's letter in 2020 and will reflect this in our 2020 annual report.

Findings

- 9.4 A focus of our inspections at SIS this year has been the adequacy of information provided to the Foreign and Commonwealth Office (FCO) in advance of and during overseas operations. Noting that the FCO has imposed certain restrictions on the format and length of what SIS can provide as briefing material to the Secretary of State, we have found that briefings have been clear and, in most cases, comprehensive. We have identified that on some occasions, particularly around changing circumstances during a live operation or where conflicting legal advice has been voiced, SIS could usefully have expanded on what was provided for consideration by the Minister. Nonetheless, we have concluded that SIS was entitled to act as they did in all the operations we have reviewed, and the Secretary of State was given adequate information to make informed judgements, in particular in relation to reliance on section 7 of the ISA and the Consolidated Guidance.

- 9.5 Our examination of internal processes and documentation at SIS in relation to section 7 warrants, which remains the most substantial operational work under our oversight, has shown a continued improvement in the quality and consistency of documentation. In this area, as in previous years, we have noted that the rigour of consideration by officers working overseas, and the advice in terms of compliance and legal discussion, is of a high standard.
- 9.6 Despite the professionalism of SIS officers and prioritisation of security and welfare arrangements for agents and covert human intelligence sources (CHIS), we have identified several weaknesses in SIS's CHIS handling model when conducting activity in the UK. This has led SIS to report several errors. We expect SIS to implement any training and structural changes necessary to ensure that internal oversight of CHIS activity is improved and that all officers involved in agent running have an adequate understanding of the requirements imposed by the Regulation of Investigatory Powers Act 2000 (RIPA) on activity in the UK, which currently appears to be inconsistent. In particular, we have highlighted inconsistent written reviews as a problem area for improvement. We made an offer for Inspectors of the Investigatory Powers Commissioner's Office (IPCO) to assist in awareness training for authorising officers, in particular, covering surveillance and CHIS under RIPA. We expect to see a focus on this area from SIS and a considerable decline in the number of RIPA errors reported in 2020.

Covert human intelligence sources (CHIS)

- 9.7 SIS conducts a minimal proportion of agent operations within the UK, or operations affecting individuals in the UK. These operations are authorised under RIPA, unlike SIS's overseas operations which are conducted under the ISA. SIS's agent running methodology has been developed over many years and applies a high level of professionalism and care in relation to individuals involved in gathering intelligence. However, because activities in and touching on the UK are less common, they are also less familiar to operational staff. Overall, although we are satisfied that SIS manages all agent cases appropriately, SIS needs to train staff to better recognise when RIPA is engaged and to authorise activity in compliance with the legislation. At present this continues to be an area where avoidable errors are being caused by human oversight (see paragraph 18.8).
- 9.8 RIPA paperwork of SIS demonstrates inconsistent written evidence of oversight and governance of CHIS activity by authorising officers within SIS. Reviews of RIPA CHIS authorisations are not always carried out in accordance with the Codes of Practice (CoP) and, whilst SIS takes agent safety very seriously, written risk assessments on these authorisations are not always as comprehensive as they could be. SIS should institute additional training to ensure its authorising officers are better able to evidence that they have met their obligations under RIPA.
- 9.9 We have noted that SIS's structure has led to limitations in how CHIS casework is handled and overseen. At present, the role of a Senior Responsible Officer (SRO) is conducted by several individuals within SIS who have responsibility for work within their business area.²¹ We believe that a single senior figure should have overall responsibility for these roles, even if the work is delegated. We have suggested that this person should be of sufficient seniority to ensure that compliance in this area is brought up to, and continues to, operate at the required standard. SIS has since actioned this recommendation and appointed an Assistant Director to the role.

21 The CHIS Code of Practice section 9.1 requires that each public authority appoints a Senior Responsible Officer and lists their responsibilities.

- 9.10 We have previously commented on the difficulties experienced by SIS in separating the statutory roles required for CHIS management, namely; the handler, controller and authorising officer. At times there are not enough officers of the right seniority to fulfil each of these roles separately within a single business area. This is because SIS is structured into small subject-specific units which are discrete for security reasons. SIS has now made changes to their guidance and practice to ensure that the controlling officer will be separate from the handler, and the authorising officer will be senior to, and in the management chain of, the handler.

Participation in criminality (PIC)

- 9.11 SIS has informed us that were it to be necessary for one of their agents to participate in criminality in the UK, this would be authorised via the MI5 PIC process. We cannot confirm the extent (if any) of such activity by SIS. However, we can state that our inspection of their CHIS casework did not identify any relevant issues and did not include any casework that was not compliant with this policy.

Juvenile CHIS

- 9.12 As noted for the other UK Intelligence Community (UKIC) agencies, we are satisfied that SIS has policies in place regarding the recruitment and running of juvenile CHIS.

Surveillance

- 9.13 SIS conducts very little covert surveillance in the UK. We found that their directed surveillance authorisation (DSA) casework set out a clear case for the necessity and proportionality of the covert surveillance. However, as we noted at MI5, the consideration recorded by authorising officers on DSA forms, as well as the internal review processes, are inadequate (see paragraph 8.15). Reviews are conducted in a sporadic and inconsistent manner and so we have recommended improvements in this area.

Property interference

- 9.14 SIS continues to conduct minimal activity in the UK under section 5 of the ISA. We examined a small number of warrants and were content that the operations outlined were necessary and proportionate and were properly authorised.

Targeted interception (TI) and Equipment interference (EI)

- 9.15 SIS uses targeted interception and targeted equipment interference (TEI) warrants and does not presently rely on bulk warrants for interception or equipment interference. We inspected SIS's use of interception and equipment interference in July 2019 and found that overall SIS demonstrated a high level of compliance with the IPA and CoP.

Thematic warrants

- 9.16 We examined a selection of thematic TEI warrants. These were broad in scope but the number of deployments under the warrants was low and each deployment was conducted under an internal approval. We were satisfied that the internal approvals we inspected contained careful assessments of necessity and proportionality. We identified a small

number of thematic warrants where the subject-matter of the warrant was problematic, for example the subject matter being defined in terms of the activity it authorises, not the activity for which the equipment is used, and another where some subjects did not fully match the description of the subject matter in the warrant. We saw similar issues on some Government Communications Headquarters' (GCHQ) warrants and so highlighted this to the Judicial Commissioners (JCs) to inform their consideration of thematic warrant applications in future. This demonstrates how improved oversight can be derived from the exchange of information between our Inspectorate and the JCs exercising prior approval under the double lock.

Warrant management

- 9.17 Following the introduction of the IPA, SIS adopted a new electronic management system for warrant applications. Transition to this system involved a manual migration of warrants and all related documentation. We anticipate that this will enable SIS to develop a tighter grip on the technical coverage in place under each warrant at any given time, ensuring that subjects or associated factors do not remain on a warrant after it is no longer necessary. We were concerned that the technical limitations of the new warrant management system mean that SIS are still carrying a greater risk of errors than is advisable. We recommended that SIS must implement robust processes to keep warrants under review and ensure that warranted activity ceases when it is no longer necessary and proportionate.
- 9.18 To date, SIS has taken steps to improve oversight of activity taking place under each authorisation, which goes some way to addressing our concerns. For example, in conversation with SIS we identified that the new electronic management system does not produce any documentation showing a clear link between the subjects of the warrant and their associated factors. This increased the risk that when a subject was removed from a warrant one or more of their factors remained on the warrant in error. SIS has developed a capability to show the relationship between the subject and factor to enable them better to manage their warrants; SIS now provides this information to support their warrant applications as required.

Computer Misuse Act offences committed by agents

- 9.19 SIS reported an error whereby an agent had been tasked to conduct activity which might constitute an offence under the Computer Misuse Act 1990 (CMA). As a result of this error, SIS sought a new thematic TEI warrant to authorise any potential criminal liability under the CMA in respect of agents obtaining data from computer systems. This will be in addition to any required specific RIPA CHIS authorisation for activity in the UK. We agree that it is appropriate for this activity, subject to the significant safeguards and restrictions explained in the application, to be authorised under a thematic authorisation. However, we will review reliance on this authorisation closely to ensure that any conduct which might breach the CMA is necessary and appropriate, and that the activity of SIS's CHIS in this area is clearly recorded and properly overseen internally.

Testing and training warrants

- 9.20 Section 17(2)(c) of the IPA provides for agencies to obtain interception warrants for testing and training purposes whilst sections 101(1)(g) and (h) provide for warrants for the testing, maintenance and development of equipment interference capabilities and training in the use of such capabilities. We are satisfied that SIS made appropriate use of IPA warrants to authorise testing and training activities during 2019.

Bulk communications data (BCD)

- 9.21 Consistent with their activity in 2018, SIS did not undertake bulk acquisition of Communications Data (CD) in 2019. SIS continue to have access to certain BCD acquired by GCHQ and MI5 where it is operationally necessary. We inspect how that data is used by SIS at the other agencies and confirm that it is lawfully obtained and that disclosure between the agencies is appropriate.

Bulk personal datasets (BPD)

- 9.22 As stated in last year's report, we inspect all appropriate records held by SIS to assure ourselves that it is necessary for SIS to retain and examine the range of BPDs they hold. We also review their data handling policies and internal compliance structures. Since transitioning to the IPA, SIS has introduced improvements to their handling control and administration of BPD. The most significant is the development of a specific panel which meets fortnightly to discuss BPD holdings. This panel, chaired and attended by SIS managers, centrally manages the retention and deletion process for BPDs and considers ways of improving compliance with the BPD provisions of the IPA within the organisation.
- 9.23 They have also introduced a monthly committee created to review systems, compliance and safeguards in relation to new and existing datasets. The new committee's remit is to:
- assess dataset compatibility;
 - ensure an appropriate level of protective monitoring is in place;
 - raise concerns or discuss development of systems; and
 - manage compliance audit.
- 9.24 This is a welcome development, which reflects the importance of prioritising compliance during systems development and testing. As is reflected in the findings of the compliance review at MI5 and the Compliance Improvement Review recommendations made by Sir Martin Donnelly (see paragraphs 8.56 to 8.58), compliance has not always been prioritised at the earliest stages of development. This can make it necessary to retrofit compliance requirements onto analytical systems or implement manual processes where it would be preferable to have automatic review of holdings. SIS has created a third panel centrally to manage the retention and deletion process, which we judge will improve compliance further.
- 9.25 SIS has a complex IT structure with several legacy record systems. SIS has undertaken a review to assess the risk that these systems might hold data which would now constitute BPD under the terms of the IPA. This work is being completed as a second layer of assurance, following a systems review which was conducted by each UKIC agency to ensure that all datasets which should be authorised under the IPA are covered by a warrant. SIS briefed the IPC on their initial findings from this review, and we expect to be briefed on the full results and any actions which SIS will take at our next BPD inspection.

Operational purposes

- 9.26 Our oversight of use of SIS BPD confirmed that their use of operational purposes is appropriate. SIS's records kept in this regard are clear and demonstrate appropriate use of this data.

- 9.27 As noted in 2018, we have seen evidence that most datasets held by SIS need to be made available to all mission areas. This is necessary to allow that data to be used most effectively and is compliant with the CoP. We therefore did not expect to see, and did not see, any requests to modify operational purposes in 2019.

Safeguards

- 9.28 Following the data compliance issues identified at MI5 (see paragraph 8.44 to 8.58) we had detailed discussions with SIS about the safeguards in place to protect their warranted data. Overall, SIS systems and processes appeared to be compliant with IPA safeguards, but we will conduct a further in-depth inspection focussing on safeguards during 2020. We expect SIS to continue to review their estate for potential risks and vulnerabilities in relation to data handling.
- 9.29 We found that the current handling arrangements introduce the risk that analysed data, which it is not necessary and proportionate to retain, is left by mission teams on the corporate records storage system. Unless manually removed, this data would persist in this system in line with SIS's corporate records policy. SIS should review their policy on how warranted data is handled and stored in their central records system. This review should ensure that no warranted data persists in the central records system when there are no longer any authorised grounds for retaining it.
- 9.30 In order to establish a higher level of assurance we have recommended that SIS should also develop a centralised record of all the processes used by mission teams for handling warranted data. This process should include consideration of how standalone systems are used: systems with no central connectivity, and which may be only used by a small number of individuals, are highly secure but are likely to require manual deletion processes. This is a potential weakness in data management if the process and policies behind this are not centrally coordinated.
- 9.31 SIS identified potential risks regarding processing of TEI warranted data in two of their tasking and processing systems at one of their facilities. We visited the facility twice during the year, first for an initial briefing and then to follow up with a more detailed briefing of the remedial work that had taken place. These risks have now been addressed. We will visit this site on an annual basis going forward.
- 9.32 We also identified, in consultation with SIS, a number of other areas for potential improvement in line with best practice. We expect to work with SIS throughout 2020 to gain assurance that all systems and environments to handle and store data obtained under investigatory powers are compliant.

Section 7 of the Intelligence Services Act 1994 (ISA)

- 9.33 Our inspections of SIS's reliance on section 7 include examination of submissions to the Foreign Secretary, which set out the proposed operation and the legal basis for conducting planned acts under the ISA. We interview officers involved in cases that we have selected for review and invariably speak to individuals working overseas on each case, as well as the central policy teams and legal advisors responsible for advising those officers. We have found in general that officers have received comprehensive training before being deployed and demonstrate a good level of awareness of the legal framework. Year on year, we have seen an improvement in the documentation of decision making by operational staff. Our 2019 inspections found that each submission is underpinned by a series of records of

meetings and decisions and email correspondence discussing operational planning and decision making. In many cases, we noted that legal advisors were routinely advising on operational actions, resulting in a high standard of compliance and consistency in approach despite SIS's dispersed working model.

- 9.34 We reviewed a range of SIS's sensitive casework and, in particular, scrutinised their reliance on broader submissions which could be applied to multiple operations. We were pleased to note that SIS provides thorough notes on the reliance on these submissions to the Secretary of State and found that SIS provided full details of certain operational acts. We judge this would enable the Secretary of State to have a full understanding of the submission. Our review of SIS's internal documentation for these submissions found that the necessity, proportionality and any risks incurred in relation to planned operations were considered and documented thoroughly on a case-by-case basis. We have suggested to SIS that this approach should be replicated for any other similar submissions that they act under.
- 9.35 SIS plays the leading role in UK intelligence work outside of the UK but increasingly cooperates with GCHQ, MI5 and the Ministry of Defence (MOD). We have attempted to follow through documentation for joint and collaborative operations between these agencies, for example reviewing internal decision making at an agency working in tandem with SIS in reliance on a section 7 authorisation. We have found that coordination between agencies has been well structured and documentation at each agency sets out complementary information; it is clear from external review what role each agency is playing and what individual and joint objectives are being met. We will continue to take this cross-cutting approach in future inspections as we believe this provides a more comprehensive picture of operational realities.

Overseas inspections

- 9.36 We inspected three of SIS's overseas stations in 2019. One of these inspections was conducted remotely via in-person discussions with the Head of Station and video-link conversations with members of his staff. We inspected one station where we understood there to be frequent cooperation with the local intelligence service in relation to terrorist activity within that country. Ahead of and during this inspection, SIS briefed us on some issues they had working with that liaison partner, which had led to a temporary suspension of cooperation. Prior to the inspection, SIS brought to our attention a situation in which they were concerned that individuals detained within the country following joint intelligence operations might be subject to unacceptable treatment. SIS drew this case to our attention providing substantial detail, including contemporaneous documentation, on this issue and the steps that they had taken to mitigate and resolve any risks. SIS demonstrated a rapid response to a potentially unacceptable situation and we are satisfied that they took all possible steps to ensure that any possible risk of harm to these individuals was minimised. SIS also demonstrated the work that had been conducted within their office to learn lessons from this issue. At the point of our inspection, SIS had renewed the relationship and demonstrated a number of active safeguards for operational working. We challenged SIS's rationale and legal basis for continuing the relationship and were satisfied that this was a decision that could be approved by the Foreign Secretary. Although SIS had briefed the Foreign Secretary on the matter, we urged them to provide updated information to the Secretary of State during any subsequent requests for approval to act under section 7.
- 9.37 During 2019, SIS were required by the FCO to restrict the length of submission documents. Although there is the option to provide additional and contextual information in an

annex, we have raised the concern that this may lead to a distortion of facts and could prevent SIS from giving a full and balanced case for appropriate ministerial oversight. We have identified one instance where we believe the paperwork submitted to the FCO was misleading in part because of the brevity imposed by the FCO, but in this case the risks were overstated and so there is no concern that any key facts were omitted or that the Secretary of State would not have authorised the case in its full reality.

- 9.38 At one station, SIS briefed us on some online operational activity which related to an assessed juvenile individual. The documentation we inspected demonstrated that the case was paused and thoroughly assessed when SIS identified that the individual might be a juvenile. This case followed SIS's policies on handling such instances, and the case for continued engagement with this individual was well set out on the record. This demonstrates the recognition of the importance of certain sensitive categories of individuals and how centrally administered training and guidance is effective globally.
- 9.39 We reviewed a section 7 submission relating to a high-risk SIS agent case overseas. SIS identified a risk that the agent may be involved in serious criminality overseas. SIS did not encourage, condone or approve any such criminality on the part of their agent. In their submission, SIS set out that they had secured the agent's cooperation on terms of full transparency about the activities in which the agent was involved. It included some clear 'red lines', setting out conduct that was not authorised and would result in the termination of SIS's relationship with the agent.
- 9.40 On renewal, six months after the original submission, SIS set out a number of indicators that the agent may have been involved in, or have contemplated, the serious criminality referenced above. We concluded that, on the basis of this new information, SIS's 'red lines' had most likely been breached, but the renewal submission failed to make this clear. Whilst the submission referred to SIS's 'red lines' provided information about criminality that may have occurred and noted an increased risk in the case, it did not make expressly clear that SIS's 'red lines' had probably been crossed. We concluded that the renewal did not provide a comprehensive overview of available information which we believe would have provided the Secretary of State with a fuller and more balanced picture. SIS immediately responded to these concerns by updating the FCO.
- 9.41 SIS conducts certain activities overseas, such as surveillance activities, with reliance on class authorisations. These authorisations, approved under section 7, will describe a type of activity and will not relate to a specific operation. We asked SIS how they ensured that reliance on those authorisations were properly documented and how they ensured that the Secretary of State had a clear understanding of the extent to which these authorisations were relied on. We were satisfied that this issue had been considered carefully by SIS's legal team. SIS does not record individual instances of reliance on these authorisations but will have operational planning documents to record the justification for, and purpose of, those actions. We understand that the Secretary of State may authorise certain common activities under the ISA in this way and were satisfied that the regular written and oral briefings provided by SIS to the Foreign Secretary provide adequate sight of their operational activities to enable him to make an informed judgement on the ongoing necessity of these authorisations. We found that SIS's internal records clearly documented the necessity and proportionality of conducting operational acts under these authorisations.

Consolidated Guidance

- 9.42 Overall, we remain impressed by the care and rigour taken by SIS in dealing with cases that engage the Consolidated Guidance, including in cases overseas posing considerable risks.

Assessing risk

- 9.43 In our 2018 report, we welcomed UKIC's decision to set up a central team to draft objective summaries of liaison partners' human rights compliance statuses to inform decisions under the Consolidated Guidance. The central team made good progress in 2018 in producing assessments for some of the more challenging priority countries, drawing on classified as well as open source material. The UKIC central team is also beginning a new project to review assurances provided by foreign liaison services. The project will collate details of assurances received, alongside the liaisons' "track record" in complying with them. This has real potential value to officers making decisions that engage the Consolidated Guidance, given the importance which is often placed on assurances as a risk mitigation.
- 9.44 However, we remained concerned that these important assessments might not always be taken fully into account by those making decisions which engage the Consolidated Guidance. In response, SIS has now introduced a policy to make it mandatory to take the central team's assessments into account, where these are available. We have also recommended that UKIC explore ways to make their conclusions available to SO15 (the Metropolitan Police Service's counter terrorism unit) and the National Crime Agency (NCA), who from January 2020 will be subject to The Principles (formally known as *The Principles relating to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees* – published on 18 July 2019, replacing the existing Consolidated Guidance from January 2020). Finally, we have recommended that the officer responsible for giving the final sign off to the content of the central team's reports should be from outside the relevant operational line management chain, to ensure that the assessments are demonstrably independent.
- 9.45 We reviewed one case in 2019 where another department did not agree with SIS's assessment of the legal risks associated with a course of action that engaged the Consolidated Guidance. The Ministerial submission did not make any reference to this difference of view and, to this extent, was misleading. We have recommended that SIS ensure that any dissenting views – whether within SIS or between SIS and other departments – are clearly set out in submissions in future.

Assurances and caveats

- 9.46 As we have noted in previous reports, assurances are an important mitigation which can be relied upon by HMG to prevent mistreatment at the hands of a liaison service. They are typically sought from a senior figure who can guarantee that an individual will be detained in a specific, compliant facility and that officers will not engage in unacceptable behaviour.
- 9.47 In our 2018 report, we noted a recommendation that SIS highlights, in Ministerial submissions, any cases where they judge assurances provided by foreign liaison to be particularly fragile. In 2019, we reviewed a number of high-risk cases where this was the case and were satisfied that SIS presented the risks associated with the proposed course of action in a clear and objective manner.
- 9.48 Caveats are often attached to intelligence passed in writing to a liaison partner setting out how the intelligence is to be used. Typically, the caveat would instruct that no action should take place on the basis of the intelligence without first consulting the UK. We have previously recommended that caveats should be clear and concise, and translated into the local language wherever possible. SIS has informed us that this requirement has been incorporated into relevant training courses and will appear in guidance to accompany The Principles in 2020.

Allegations of mistreatment

- 9.49 We reviewed a small number of cases where SIS was made aware of allegations of mistreatment by a liaison partner in circumstances which engage paragraph 6 of the Consolidated Guidance. In every case, we were satisfied that SIS conducted a full and thorough investigation as far as was reasonably practicable. None of these cases involved Her Majesty's Government (HMG) making a material contribution to any mistreatment which may have occurred. Where relevant, SIS's investigations included an assessment as to whether the allegations, if found to be credible, might impact on their own work with foreign liaison partners in country.

Case study: allegations of mistreatment

In the course of a joint operation run by the Secret Intelligence Service (SIS) with a foreign liaison partner, a terrorist suspect was arrested and subsequently put on trial. The suspect was eventually acquitted and released. SIS then received the text of the court judgment, which included reference to allegations made by the suspect that he had been subjected to mistreatment during his time in detention.

It is not uncommon for suspects to make such allegations in the course of criminal trials as part of their defence strategy. Nevertheless, senior SIS staff met the leadership of the foreign liaison service shortly after SIS became aware of the allegations, pressing them to conduct a full investigation. Under the circumstances, and taking into account the difficult political and operational environment in which this case arose, we were satisfied that SIS had taken all reasonable steps to investigate the allegations once they became aware of them.

Unsolicited intelligence

- 9.50 We reviewed a case in which SIS received intelligence, sourced from a detainee in a particularly high-risk country, which posed questions about UKIC's policy on the receipt of unsolicited intelligence.²² In this case, SIS applied the UKIC policy on receipt of unsolicited intelligence which was agreed with the FCO and the former Intelligence Services Commissioner in 2016. This policy provides that:
- The "serious risk" threshold at which UKIC would notify Ministers if seeking to solicit a detention, or feed in questions to a detainee, did not need to be applied in the case of unsolicited reporting. Instead, UKIC would inform Ministers following receipt of credible reporting leading to the knowledge or belief that a specific detainee, from whom UKIC received unsolicited intelligence via a third party, had been subject to unacceptable conduct.
 - UKIC will consider in any case where there was *specific knowledge or belief* that unacceptable conduct had taken place, whether continued receipt of the intelligence was an encouragement of the means used to obtain it.
- 9.51 Having reviewed the policy in the light of this particular case, we were satisfied that this is a legitimate interpretation of the word "believe" in para 27 of the Consolidated Guidance.

22 Paragraph 27 of the Consolidated Guidance provides that *"...in the cases where personnel receive unsolicited intelligence from a liaison service that they know or believe has originated from a detainee, and which causes them to believe that the standards to which the detainee has been or will be subject are unacceptable, senior personnel must be informed. In all cases where senior personnel believe the concerns to be valid, Ministers must be notified of the concerns."*

In this particular case, SIS's internal records suggest that SIS did have specific knowledge or belief that the detainee would have been denied due process. As such, per the terms of the 2016 policy, Ministers should have been notified, even though SIS was not seeking to feed in questions to be put to the detainee.

Non-compliance with the Consolidated Guidance

- 9.52 We reviewed one case in which SIS did not fully comply with the Consolidated Guidance, and a second where we concluded SIS had not complied with the spirit of the Guidance. In one case, which SIS brought to our attention, SIS officers working in Country A failed properly to consider the conditions to which a detainee may have been subject following his detention in Country B. They also did not consider the lawfulness of the detainee's transfer from Country B to Country A. We were satisfied that, following this failure, SIS has taken appropriate steps to prevent similar non-compliance occurring in future, including a reminder to relevant staff of the applicable SIS policies. In the event, following an investigation by SIS, there were no concerns about the way in which the detainee in question had been treated. We concluded that part of the root cause of the problem was an understandable confusion amongst operational staff about what is, in fact, permitted by the patchwork of applicable submissions and authorisations. We have therefore recommended that SIS ensures that all relevant staff overseas fully understand exactly what is authorised by the relevant permissions.
- 9.53 In a separate case, SIS covertly obtained intelligence sourced from the debriefing of a detainee. The material obtained by SIS included clear indications that the detainee had been mistreated by a foreign liaison service. Whilst the Consolidated Guidance does not explicitly govern the covert acquisition of intelligence sourced from detainees, the spirit of the Guidance was, in our assessment, certainly engaged and SIS should have had regard to it. SIS did not do so because they did not believe that the Consolidated Guidance (either by its letter or its spirit) applies in this sort of scenario. In our view, had SIS had regard to the spirit of the Consolidated Guidance, then they should have concluded that whilst in practice there was nothing SIS could have done to prevent any future mistreatment or to raise concerns with the detaining authority before seeking to obtain the debrief material, SIS should have submitted to Ministers before seeking to obtain the material given the serious risk the detainee may have been subject to mistreatment (as, in the event, the debrief material made clear once this was obtained).

10. Government Communications Headquarters (GCHQ)

Overview

- 10.1 We conducted a series of inspections at GCHQ and received briefings on key areas of their work during the course of 2019. These discussions, and our oversight, focused on the transition to the new legislation for GCHQ's more technical work and we were grateful for the involvement of the Technology Advisory Panel (TAP) in this. Because of GCHQ's functions, there is a greater focus on technically complex activity and bulk collection, as is reflected in this chapter, and GCHQ has taken a leading role in discussions with the Investigatory Powers Commissioner's Office (IPCO) and government stakeholders throughout the year to ensure that these are well managed and well understood by overseers, including our Judicial Commissioners (JCs).

Findings

- 10.2 The Investigatory Powers Act 2016 (IPA) has formalised provisions for conducting operations in bulk. A key question for us is whether the bulk powers are balanced appropriately with targeted powers and we felt on examination that this was well considered and well handled by GCHQ. Overall, we were satisfied that operations conducted under the bulk warrants were necessary and proportionate, but the quality of applications for internal approval was variable and we observed that there was room for improvement in the way that such applications were set out.
- 10.3 In our 2018 report, we noted that a higher number of GCHQ's equipment interference (EI) operations were relying on bulk equipment interference (BEI) warrants than had previously been envisaged. This continued to be the case during 2019, when GCHQ successfully applied for new BEI warrants relating to work that was previously authorised through different mechanisms. GCHQ also has plans to apply for a small number of BEI warrants in 2020. We will be engaging with GCHQ at an early stage to determine how best to provide ex post facto oversight of these new bulk warrants.
- 10.4 We found that the critical role of bulk communications data (BCD) to the range of activities conducted at GCHQ was well articulated in the casework we inspected. We considered the nature of the requested data and the stated intelligence requirements and were satisfied that the documentation demonstrated that their approach was necessary and proportionate.
- 10.5 Our inspections of covert human intelligence sources (CHIS) and directed surveillance at GCHQ also found a good level of compliance, but we saw only partial improvement against previous recommendations. Following our 2019 inspection, GCHQ will provide an action plan for improvement to CHIS and directed surveillance applications (DSA) processes. This activity comprises a small but important part of GCHQ's covert activity online.

Covert human intelligence sources (CHIS)

- 10.6 CHIS operations play a small but important role in support of GCHQ's functions. All the CHIS activity authorised under the Regulation of Investigatory Powers Act 2000 (RIPA) by GCHQ is carried out by officers online. We examined a small number of CHIS cases this year and found them to be necessary and proportionate.
- 10.7 We made several recommendations following our 2018 inspection. These were predominantly regarding the role of the Authorising Officer (AO). We also made a recommendation, similar to that made at MI5 (paragraph 8.8), that authorisations which relate to officers carrying out activity online should relate to the planned activity rather than the persona or profile, which could be used by multiple officers to interact with several individuals online. GCHQ have developed new authorisation forms and engaged external training providers. Training for officers and controllers has been included in a formal 'learning path' and GCHQ has written a new CHIS policy handbook for its staff. As a result of these changes, the welfare of the online operatives is now more formalised by means of psychological assessments, workshops and surgeries, but further work is still required to ensure that detailed, operative specific risk assessments are completed in every case.
- 10.8 Taken together we believe that these measures should address the shortcomings previously identified and provide a solid foundation for CHIS activity. However, delays in implementation meant that none of the intended improvements were evident in the records examined this year. Given the ongoing improvements, we did not make additional recommendations, but have offered to support internal training courses in the future.
- 10.9 At our most recent inspection, GCHQ were unable to locate and produce some of the supporting records around case management and welfare that we asked to see. We have asked GCHQ to improve their housekeeping and ensure that they are able to present the required documents at future inspections.

Juvenile CHIS

- 10.10 We are satisfied that GCHQ has policies in place regarding the recruitment and running of juvenile CHIS.

Surveillance

- 10.11 GCHQ uses directed surveillance to conduct online activity and examine communications devices which might have been remotely interfered with by hostile actors. A device can be examined with the owner's consent, or where it is necessary to examine communications on the device, with the additional consent of one of the parties to any communication and a directed surveillance authorisation under RIPA (see section 44(2) IPA). We have discussed the legal framework for this activity with GCHQ and have found their records in relation to these operations and activities to be of a generally high standard. Nevertheless, GCHQ reported 3 errors relating to surveillance in 2019. These errors stemmed from a lack of understanding of when an authorisation is required and of the need for unambiguous consent from the recipient or sender of messages when one-party consent procedures are relied on. GCHQ recognise these issues and we expect to see a reduction in errors in 2020.
- 10.12 Although some of the online activity authorised was broadly drawn, we found all authorised to be necessary and proportionate. We have observed that broadly drawn applications require those working on them to place a greater emphasis on necessity and

proportionality considerations. Such applications require a greater level of consideration to be documented on internal records: the intended methodology should clearly be recorded, as well as the anticipated scale of the activity, so that the AO can make a fully considered decision. In some cases, we felt that GCHQ could legally conduct planned operations without authorisation under RIPA and so we questioned whether some of the online conduct being authorised by GCHQ required a directed surveillance authorisation (DSA). We noted that any DSA casework produced in these debatable cases must still be of a high standard.

- 10.13 It was disappointing that only limited progress had been made in relation to previous recommendations regarding the lack of written input from AOs. GCHQ's forms for initial authorisation and renewal of directed surveillance do not provide space for AOs to comment on the necessity, proportionality or collateral intrusion. The scope for improvement is limited until these forms are redesigned.
- 10.14 We also saw little improvement in review procedures for existing authorisations, which are required under the Code of Practice (CoP). GCHQ has provided additional guidance and training but this is not yet widely evident in the authorisations scrutinised. We have offered to assist GCHQ in providing further training or awareness sessions for authorising officers.

Property interference

- 10.15 GCHQ conducted very little activity under section 5 of the Intelligence Services Act 1994 (ISA) in 2019. During our inspection we reviewed casework for a small number of warrants and received briefings from the teams working under those authorisations. We were satisfied that each warrant was necessary and proportionate and that the considerations in each case were well set out.

Targeted equipment interference

Use of general descriptors

- 10.16 We examined a number of thematic warrants where a general descriptor had been used (see chapter 2). We found that the explanation of why it was not reasonably practicable to name or describe all the individuals was not well made on two general descriptor warrants we examined. We observed that a clear and rational explanation must be made with respect to this matter in all relevant thematic warrants and must be set out clearly for these two warrants at renewal. We noted similar issues at SIS and several law enforcement agencies (LEAs) and expect this to be rectified as applicants become more familiar with the application templates and requirements of the legislation and CoP.
- 10.17 We noted that GCHQ was making use of set descriptions of conduct to be authorised in EI warrant applications and renewals, although in some cases not all described conduct was intended or necessary and a more narrowly defined description of the conduct could have been used without jeopardising the operational utility of the warrant. Although the more limited conduct which GCHQ intended to carry out was made clear in the body of the applications, the more extensive description of conduct appeared on the schedule to the warrant. GCHQ explained that the description of conduct to be authorised was contained in a form of words on a template that had been mandated by the Home Office. Our enquiries with the Home Office revealed that this was not the case and that GCHQ were not bound by the forms of words in template documents. GCHQ's template has now been updated. There is no suggestion that any unnecessary conduct occurred under these warrants.

Development, testing and training

- 10.18 Sections 101(1) (f), (g) and (h) of the IPA introduced specific categories of warrant for training and testing. We would expect these to be used thematically, covering a type of training or type of equipment under development. We were briefed by GCHQ on certain testing, training and development activity with respect to targeted equipment interference (TEI).²³ We were satisfied that this activity was necessary and being used in a proportionate manner.
- 10.19 In our 2018 report, we commented on the quality of GCHQ's Records of Reliance with respect to certain activities undertaken by contractors and industry partners conducted under section 5 of the ISA. This activity is now conducted under one of the IPA TEI warrants referred to above. GCHQ have subsequently improved the way in which they record such activity.

Targeted examination warrants (TXEI)

- 10.20 Targeted examination warrants are required to select for examination protected material obtained under bulk warrants when the target is known to be in the British Islands. Continuity of Coverage Authorisations (CCA) are obtained to allow the selection for examination of such material to continue for a limited period when a subject previously believed to be overseas is found to be in the British Islands. The CCA is valid for a period of five working days, by which time the agency must have either obtained a TXEI warrant or ceased selection for examination using selectors authorised under the bulk warrant. We were satisfied with the way that GCHQ was managing TXEIs and CCAs and we found that GCHQ seeks to rely on a TXEI when a British Islands connection cannot be ruled out, which represented best practice in this area.

Bulk equipment interference (BEI)

- 10.21 We received briefings on various EI techniques during inspections and bespoke sessions. We welcome this level of engagement in what is a complex area. GCHQ warrant applications and renewals were generally completed to a high standard with often complex technical issues clearly explained.
- 10.22 A large proportion of GCHQ EI operations are conducted under bulk authorisations. We are content that it is still appropriate for GCHQ to continue to authorise these activities through bulk warrants especially given the additional safeguard of necessity and proportionality being addressed at the point when they can be most accurately assessed. Given the scale of the activity being approved internally, we will continue our enhanced ex post facto oversight as described above. We will take the same approach with internal approvals under all new and proposed BEI warrants and subject these to close scrutiny at future inspections. We are satisfied that GCHQ continue to consider carefully on a case-by-case basis whether it is most appropriate to authorise EI activity under bulk or targeted warrants and we will continue to pay close attention to this both during our consideration of warrant applications under the double lock and at inspections.

23 Section 101(1) sets out the subject matter that is permissible for targeted equipment interference. 101(1)(f) relates to equipment which is being, or maybe, used for the purposes of a particular activity or activities of a particular description; 101(1)(g) relates to equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information. 101(1)(h) relates to equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment.

- 10.23 We recommended that all applications should consistently and explicitly record the link between the target and a statutory purpose and intelligence requirements. We also recommend that all applications should clearly address the potential for collateral intrusion and relevant mitigations when assessing proportionality. We identified particular need for improvement in one business area. We looked into the issue more closely during our second inspection in 2019 and noted some progress, but there is still room for improvement. We observed one other case where a targeted individual did not match the description given in the application and will continue to pay close attention to this area at future inspections.

Operational purposes

- 10.24 GCHQ may only select for examination material obtained through bulk equipment interference for one of the operational purposes listed on the warrant. We are satisfied that GCHQ's use of operational purposes with respect to the examination of material obtained through EI is appropriate.

Additional measures imposed by the Secretary of State

- 10.25 Most bulk authorisations are granted against the full range of available operational purposes to allow any intelligence obtained to be used effectively by the requesting agency.²⁴ In renewing two GCHQ BEI warrants, the Secretary of State required to be consulted prior to any proposal to undertake activity in support of a small number of those operational purposes. We endorse the Secretary of State's requirement to be consulted by GCHQ, which creates an additional safeguard in the form of ministerial oversight and ensures that the minister is well sighted where the necessity and proportionality of specific operational activities may be particularly finely balanced.

Bulk interception

- 10.26 As noted in chapter 2, in September 2018 the European Court of Human Rights (ECtHR) handed down its judgment in *Big Brother Watch v. UK*. Whilst the case is pending the result of an appeal hearing before the Grand Chamber, the judgment included a number of findings which are relevant to our oversight of bulk interception and which, in consultation with GCHQ, we have factored in to our planning for future inspections.
- 10.27 In particular, in relation to the bulk interception regime under RIPA which has since been replaced by provisions in the IPA, the Court was:

"not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, however, is the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications." (paragraph 347)

24 Section 178 of the IPA requires that a bulk equipment interference warrant must specify the operational purposes for which any material obtained under the warrant may be selected for examination. The CoP section 6.6 states that it is highly likely that a bulk equipment interference warrant will specify the full range of operational purposes (in accordance with section 183(6)) of the IPA.

- 10.28 This finding echoed a similar recommendation in the Intelligence and Security Committee's *Privacy and Security: A modern and transparent legal framework*²⁵ report of March 2015. We therefore conducted a review of our approach to inspecting bulk interception in 2019, which included a careful review of the technically complex ways in which bulk interception is actually implemented. As a result of this review, the findings of which have been agreed with GCHQ, our inspections of bulk interception from 2020 onwards will include a detailed examination of the selectors and search criteria alluded to above by the ECtHR. The exact format of this inspection is yet to be agreed and like our other inspections will be the subject of continuous review.

Operational purposes

- 10.29 GCHQ may only select for examination material obtained through bulk interception for one or more of the operational purposes listed on the warrant. We are satisfied that GCHQ's use of operational purposes with respect to the examination of material obtained through bulk interception is appropriate, including the addition through modification of an operational purpose to correct an earlier omission.

The Equities Process

- 10.30 The Equities Process is the means through which decisions are taken on the handling of vulnerabilities found in technology to achieve the best overall outcome in the interests of the United Kingdom. In November 2018, GCHQ publicly avowed the Equities Process and confirmed that IPCO would oversee how the process operates in practice, with the aim of providing public reassurance.²⁶ Whilst carrying out operational activity, analysts working at GCHQ or elsewhere within government may identify vulnerabilities in technology. These vulnerabilities may represent a risk to the security of the UK or its allies. In some cases, the same vulnerabilities might provide a means by which UKIC could obtain intelligence in pursuit of its statutory functions. The term "equity" in this context is used to refer to a vulnerability known to GCHQ.
- 10.31 Under the Equities Process, GCHQ must decide whether a vulnerability should be disclosed or kept secret. GCHQ applies objective criteria to decide whether a vulnerability should be released to allow it to be mitigated or retained so that it can be used for operational purposes. The starting position is always that disclosing a vulnerability will be in the national interest.
- 10.32 The decision-making process involves:
- The Equities Technical Panel (ETP), made up of subject matter experts from across UKIC;
 - The Equity Board (EB), which includes representatives from other Government agencies and Departments as required. The EB Chair is a senior civil servant, usually drawn from the National Cyber Security Centre (NCSC), and is answerable in this role to the Chief Executive Officer (CEO) of the NCSC. We observed an EB meeting in 2019 and will be observing at least one further meeting in 2020; and
 - The Equities Oversight Committee (EOC), chaired by the CEO of the NCSC, which seeks to ensure the Equities Process is working appropriately. The EOC may also consider equity decisions that have been escalated to them by the EB.

25 Intelligence and Security Committee of Parliament, "Privacy and Security: A modern and transparent legal framework" (2015), <https://bit.ly/3nuFWWu>

26 GCHQ, "The Equities Process" (November 2018), <https://www.gchq.gov.uk/information/equities-process>

- 10.33 Currently, our oversight of the Equities Process is being conducted on a non-statutory basis. We expect the Government to keep this under review but will continue to conduct oversight of this important process.

Inspections of the Equities Process

- 10.34 We conducted two initial visits to GCHQ in 2019. During these two visits, we were briefed in detail on how the Equities Process works in practice and familiarised ourselves with the processes and concepts involved. We made some initial recommendations to GCHQ, which were focused on gathering further information and identifying areas which require more detailed investigation in 2020. We also made a number of recommendations about how the decision-making process itself could be improved. Whilst we saw evidence that GCHQ is making careful, evidence-based decisions about individual vulnerabilities, we queried the extent to which GCHQ is assessing the aggregate risk of these decisions over time. Where relevant, Equities Process decisions should refer explicitly to NCSC assessments about cyber risks where this is relevant to the risk of retaining the vulnerability in question.
- 10.35 Our other key recommendation in 2019 was for GCHQ to consider how ministerial oversight of the Equities Process could be improved. We expect to see GCHQ's first annual report on the Equities Process, which will be addressed to the Foreign Secretary, in due course. We have also underlined to GCHQ the importance of ensuring the Foreign Secretary can exercise his duty, under section 2 of the IPA, to have regard to the public interest in the integrity and security of telecommunication systems. This should include the extent to which the Foreign Secretary needs to have sight of GCHQ's judgements about the impact decisions taken under the Equities Process may have on such systems.

Bulk communications data (BCD)

- 10.36 One GCHQ bulk acquisition warrant which relates to several telecommunication operators commenced in February 2019 and has been renewed since. Similar to MI5 (see paragraph 8.35), GCHQ has a system used by their analysts to outline why the examination of specific data is both necessary and proportionate. This allows subsequent examination or audit of the activities of specific members of staff who are authorised to undertake the examination of BCD. These records will also include details of any sensitive information, such as that relating to sensitive professions, which might be examined. Through our inspections, we concluded that GCHQ's recorded justifications to undertake the examination of BCD were of a good standard and satisfied the principles of necessity and proportionality. We were satisfied that no unnecessary examination of sensitive material is being made.
- 10.37 As we explained in the 2018 report, we made recommendations as to how the training and guidance provided to analysts could be delivered to highlight the requirement for clarity within their justifications. This could be done, for example, by using simple text setting out what operational benefit is sought when undertaking the queries. We are satisfied that training, and awareness of the requirements set out in the CoP, is now maturing, and that the justifications being recorded by the analysts are detailed and yet concise.
- 10.38 GCHQ's Internal Compliance Team carries out robust retrospective audit checks of the analysts' justifications for the selection of BCD. When the internal audit team identify that necessity or proportionality justifications recorded by particular analysts are below the minimum requirements, the Policy and Compliance Lead is responsible for ensuring that the analyst is made aware. The Policy and Compliance Network is a network of staff distributed throughout GCHQ who are responsible for compliance in their areas.

This includes working with analysts to ensure their justifications are up to standard and providing additional training when audit has found justifications which fall below requirement. Importantly, GCHQ were able to demonstrate how this process works when submissions fall short of the required standard.

- 10.39 Before our inspection, we worked with GCHQ's Internal Compliance Team to select several hundred records from the system which we then examined to review the analysts' necessity and proportionality justifications for the selection of BCD. During the inspection, we spoke to the Internal Compliance Team to discuss the findings and outcomes. We concluded that the analysts had properly justified in each case why it was necessary and proportionate to access the BCD.
- 10.40 In addition, GCHQ's IT Security Team conducts technical audits to identify and further investigate any areas of concern. This will include any activity that may be a breach of the operational requirements. The senior managers we interviewed as part of the inspection process explained and demonstrated in some detail how the audit processes work and the function of the team. We were satisfied with the thorough overall approach.

Sharing bulk data: Review of procedures at GCHQ

- 10.41 In our 2018 report, we explained that, in *Privacy International v GCHQ & Others IPT/15/110/CH*, the investigatory Powers Tribunal (IPT) had considered the lawfulness of GCHQ's use of certain bulk data. The IPT judgment, published on 23 July 2018, called for "a review of existing procedures at GCHQ in relation to sharing of intelligence and of bulk datasets... under the supervision of IPCO". In response, GCHQ conducted a detailed review of the processes and procedures governing decisions to share data in bulk with foreign partners and then implemented measures to bring about improvements. In the future, this area will be covered as part of our regular oversight and inspection arrangements.
- 10.42 One significant challenge the review faced was the commencement, in August 2018, of the parts of the IPA relating to the various bulk powers. This included the implementation of the safeguards contained in the Act, the accompanying Codes and the involvement of JCs undertaking the double-lock of bulk warrants. This includes the requirement under the IPA that, before approving the sharing of material obtained as a consequence of conduct under a bulk warrant, the Secretary of State must be satisfied (to such an extent (if any) as the Secretary of State considers appropriate) that the overseas authority with whom material is being shared has in place safeguards in relation to retention, disclosure and examination. In our supervisory role, we considered the adequacy of GCHQ's assurances to meet this requirement.

Summary of outcomes from the review

- 10.43 The main outcomes of GCHQ's review are as follows:
- Sharing of bulk data with foreign intelligence partners is now incorporated into our regular oversight and inspection processes;
 - The review has brought new standardisation. Decisions and permissions to share are captured on a Data Sharing Permission (DSP) form and stored electronically in a central location;
 - Each DSP records the necessity and proportionality of sharing a type of bulk data with the partner in question and how the partner safeguards operational data, confirms that

- the relevant bulk (interception, equipment interference, personal data & BCD) warrant permits overseas sharing, and also details the accesses covered and equity considerations;
- Each foreign partner has provided written assurance in relation to their handling of shared bulk data;
 - A dedicated team is the formal coordination point and record keeper of DSPs for the sharing of bulk data with Five Eyes and other foreign partners; and
 - GCHQ has invested in the development of a workflow tool to automate the DSP process by marrying operational data sharing in their systems to the DSPs. This provides a double-check capability that mitigates the risk of sharing without permission. An additional feature is the ability automatically to match warrants to operational purposes, thus reducing the burden on those checking that the appropriate operational purpose/s are present and correct.
- 10.44 We anticipate that the measures taken by GCHQ including the automated workflow tool, when implemented, will improve compliance in this area. They will provide a centralised record of what data is shared with whom, where and why. The decisions about sharing will be accessible by GCHQ staff as required, by our inspectors and, when necessary, by the IPT and will meet the requirements described in the Tribunal's CLOSED judgment on the Privacy International case in July 2018.

Bulk personal data (BPD)

- 10.45 Overall, administration of bulk personal datasets (BPDs) within GCHQ is to a high standard. During this reporting period GCHQ introduced a clear and auditable process when considering the classification of BPD. All decisions and details of the datasets are collated internally and recorded in an auditable manner. We intend to review this material at future BPD inspections.
- 10.46 As explained in paragraph 10.38 GCHQ has introduced an enhanced compliance team. This team carries out retrospective audits of the justifications used to examine BPDs and provides individual support via a network of staff who volunteer to assist the compliance team. The members of staff who represent the Policy and Compliance Network (PCN) are responsible for compliance with the IPA in their work areas or teams. They engage with the central compliance unit and act as a conduit when, for example, an analyst's justification falls below standard. The PCN also trains staff and acts as mentors. We have commended this approach, which we believe will ensure a good level of compliance across the agency.
- 10.47 In our last annual report, we highlighted recommendations in relation to providing staff with additional training and guidance on the examination of BPDs. Prior to inspection, we work with the compliance team to randomly select several hundred records used to justify the examination of BPD by GCHQ officers. Unlike at MI5, each record will relate to a single search conducted by GCHQ staff. The compliance team's role is to identify any inadequate justifications; if staff were suspected to be searching against BPD without the right justification for doing so, we would expect staff to be interviewed and, if necessary, appropriate action taken.
- 10.48 We examine these records, consider whether the compliance team are applying adequate scrutiny to their review and advise on whether the threshold for further investigation or breach are appropriate. In March 2019, we determined that 50% of the justifications for bulk acquisition warrants that were reviewed by the GCHQ compliance team did not meet the required standard. This was, rightly, seen to be a serious issue and the compliance team

had begun work to investigate the problem and retrain staff to improve this standard. The refreshed training on the IPA provisions and the additional training provided by PCNs have improved GCHQ's compliance in this area. We do not expect to see a slip in this standard at future inspections but will continue to review this area closely.

Safeguards

- 10.49 We conducted a bespoke inspection at GCHQ to examine safeguards for data obtained under warrant in May 2019. The primary focus of this inspection was a detailed briefing on the approach taken by GCHQ to technical safeguards across systems which handle such data. GCHQ has an agreed set of principles to which any system designed to handle operational data (including data obtained under warrant) must adhere. These principles are known as the Principles for Operational Data Systems (PODS).
- 10.50 It is the responsibility of a system developer or owner to ensure that their system adheres to the PODS. Having reviewed the PODS in detail, we were satisfied that they cover, in a comprehensive way, the obligations which apply to GCHQ's handling of operational data under the IPA. In addition, in preparation for implementation of the IPA, GCHQ undertook an extensive amount of work in assessing system compliance with the requirements of the Act, allocating around 20,000 hours of staff time in total. One of the outcomes of this work was a comprehensive list of all systems in use across GCHQ which handled data obtained under warrant. Complementary processes (contained within the PODS) mean that any new systems must be recorded in a central register. As such, GCHQ now has reliable processes that enable a centralised record of systems which handle operational data. The responsibility for the compliance of these systems rests with the system owner.
- 10.51 On the basis of material provided to us by GCHQ, including an outline of the measures taken by GCHQ to ensure it was not carrying additional compliance risk as a result of having shared data with MI5 which was being stored in Technology Environment 1 (TE1), we were satisfied that GCHQ did not have a systemic compliance issue akin to the problems identified at MI5 with TE1 (see chapter 8). Nevertheless, we will revisit this technically complex area in greater depth on future inspections to review GCHQ's safeguards arrangements.

Section 7 Intelligence Services Act 1994 (ISA)

- 10.52 In our 2018 report, we stated that the majority of the work that GCHQ historically conducted under section 7 of the ISA, which authorises activity outside of the British Isles, is now conducted under Parts 5 and 6 of the IPA. This continues to be the case. Section 7 is now relied upon by GCHQ to conduct operations which do not acquire communications, equipment data or other relevant information under the IPA. We have worked with GCHQ throughout the period of transition to the IPA to ensure that all operations are fully and appropriately authorised, particularly so that the JCs and Inspectorate have a clear understanding of how the operation is conducted and what level of interference with any individual(s)' privacy results. We have been pleased by the proactive approach that GCHQ continue to take in briefing our teams and we have a high degree of confidence that section 7 is being used appropriately and that operations are being conducted with minimal collateral intrusion.
- 10.53 We reviewed casework and internal approval documentation for section 7 authorisations as part of a broader inspection of equipment interference operations. This gave us the opportunity to discuss with GCHQ how they were managing the delineation of IPA and ISA

authorisations and to ensure that the overseas scope of any technical operations was clear. Our inspections did not identify any concerns about GCHQ's technical operations.

Consolidated Guidance

- 10.54 We reviewed a range of requests engaging the Consolidated Guidance which had been made of GCHQ by foreign liaison services, to share GCHQ-produced intelligence with other foreign liaison partners. We observed evidence that GCHQ carefully considered the risks before granting permission for intelligence to be shared in such cases, including by referring to relevant sources of evidence both on the compliance risks in the country concerned and any assurances provided by the liaison service making the request.
- 10.55 The internal process in force at GCHQ, supplemented by additional considerations made by policy and legal staff where required, is securing a high level of compliance with the requirements of the Consolidated Guidance. The way in which GCHQ records its considerations under the Consolidated Guidance provides a clear narrative of how the decision to approve or reject a request was arrived at. We made no recommendations relating to the Consolidated Guidance at GCHQ in 2019.

11. Ministry of Defence

Overview

- 11.1 We conduct oversight of the Ministry of Defence's (MOD) use of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) in the UK, and non-statutory oversight of the MOD's agent running and surveillance activities overseas. We did not conduct a non-statutory inspection of overseas activity in 2019 but will do so in February 2020.

Findings

- 11.2 The MOD continues to make limited use of investigatory powers in the UK. Based on our examination of their records and discussions with applicants, Authorising Officers (AOs), policy and legal advisors, we are satisfied that the MOD takes great care when using investigatory powers and continues to demonstrate a high level of compliance. We continue to see high quality advice from policy and legal advisors.

Covert human intelligence sources (CHIS)

- 11.3 The MOD did not conduct any CHIS activity in the UK during the period under review. We will examine the overseas use of CHIS during our next inspection in February 2020. In general, it is worth noting that the CHIS casework at the MOD is typically of a high standard.

Juvenile CHIS

- 11.4 We are satisfied that the MOD has policies in place regarding the recruitment and running of juvenile CHIS.

Surveillance

- 11.5 The MOD undertakes some directed surveillance activity in the UK. Authorisations were thorough with applicants setting out the necessity and proportionality cases in detail. Applicants and AOs demonstrated careful consideration of the potential for intrusion and surveillance operations were planned and run in such a way as to keep collateral intrusion to a minimum. We made two recommendations to address minor procedural issues. We consider that the MOD takes a very cautious approach when deciding whether to seek RIPA authorisations to cover the development and testing of new surveillance capabilities.

Interception and Equipment Interference (EI)

- 11.6 The MOD may apply to the Secretary for Defence to conduct activities in the UK which fall under the IPA, such as interception and equipment interference (EI). Under section 17(2) (c) the MOD may apply for a warrant to intercept communications for the purpose of training and testing in the UK. Similarly, the MOD may apply for a warrant to conduct EI under section 101(1)(g) for testing, maintaining or developing capabilities and 101(1)(h) for training. In our 2018 Annual Report we stated that we had discussed the provisions for thematic warrants in relation to training and testing equipment with the MOD. During 2019 we were able to examine their reliance upon these provisions.
- 11.7 The MOD has a very thorough and detailed process for internally authorising and tracking warranted activity. The MOD's authorisations were completed to a high standard and all the personnel we spoke to from various branches of the Armed Forces were well versed in the relevant legislation and had a good grasp of necessity, proportionality and collateral intrusion.
- 11.8 The MOD's internal documentation regarding the retention and deletion of warranted material is comprehensive but would benefit from greater reference to the Codes of Practice (CoP). We recommended that the MOD draws up a formal stand-alone safeguards document for material obtained under warrant and that this should be approved by the Secretary of State.

Consolidated Guidance

- 11.9 Overall, we were satisfied that the MOD is assessing risk in line with the Consolidated Guidance in a detailed and careful manner.

Assessing risk

- 11.10 In our 2018 report, we noted the requirement for risks to be quantified as either above or below the "serious risk" threshold set out in the Consolidated Guidance; officers should not fall back on "unknown risk". In 2019, we identified a number of the MOD assessments which recorded the level of risk as "unquantifiable", or which stated that the risk "cannot be said to be less than serious". These are potentially misleading phrases and should be avoided. We have recommended that the MOD ensures that all future assessments clearly set out whether the level of risk, having taken all mitigations into account, is above or below the "serious risk" threshold (or, now that The Principles have come into force, "real risk").
- 11.11 Separately, we identified a number of areas in which the forms used by the MOD to record assessments made under the Consolidated Guidance could be improved, by ensuring the questions asked of officers completing the form are as clear and unambiguous as possible.

Unsolicited intelligence

- 11.12 The Consolidated Guidance requires that, where the MOD receives unsolicited intelligence that originates from a detainee and where they believe the standards to which that detainee has been or will be subject to are unacceptable, Ministers must be notified. We identified two cases where the MOD failed to notify Ministers, only doing so months later after the initial failure to notify had been spotted. The correspondence we reviewed made

clear that the Minister for the Armed Forces took this failure seriously; he requested that changes be put in place to ensure any future cases are reported to him promptly.

Allegations of mistreatment

- 11.13 We reviewed a number of cases in which individuals alleged that they had been mistreated. We concluded that the MOD was investigating allegations of mistreatment as thoroughly as the circumstances permitted. We have recommended that the MOD should make clear in submissions the extent to which they are able to assess whether any allegations of mistreatment might indicate a systemic problem. Any conclusions should be caveated appropriately to take account of how much evidence is available to the MOD.

Training, advice and assistance operations

- 11.14 We discussed with the MOD whether the Consolidated Guidance is ever engaged when British Forces are engaged in training, advice and assistance (TAA) missions overseas. Whilst these missions do not involve the direct involvement of British personnel in detention operations, the MOD is nevertheless providing capacity building to foreign military units who may go on to detain, and potentially mistreat, individuals.
- 11.15 Following correspondence with the MOD, we are satisfied that TAA operations do not engage the Consolidated Guidance, as the MOD is not passing intelligence to a foreign authority where detention is the intended or likely outcome. Any compliance risks associated with TAA operations are governed by the Government's Overseas Security and Justice Assistance (OSJA) policy, which is not subject to oversight by the Investigatory Powers Commissioner's Office (IPCO).

12. Law Enforcement Agencies and Police

Overview

- 12.1 In 2019, we inspected all territorial forces within the UK, including Regional Organised Crime Units (ROCs) and Counter Terrorism Policing Units, together with other police forces and law enforcement agencies including the British Transport Police, Ministry of Defence Police, Royal Air Force Police, Her Majesty's Revenue and Customs (HMRC), the National Crime Agency (NCA) and Immigration Enforcement and Border Force. We also inspected covert activity of the Sovereign Based Area Police in Cyprus and the overseas covert human intelligence sources (CHIS) activity conducted by UK law enforcement agencies (LEAs), which included meeting their partner agencies in the US.
- 12.2 We conduct additional inspections if we have concerns or note repeated poor performance. We conducted four additional inspections in 2019, one of which was followed up personally by the Investigatory Powers Commissioner (IPC), then Sir Adrian Fulford, through a meeting with senior officials. One re-inspected Force had been subject to five inspections since 2016. Many of the issues raised in this year's report have featured repeatedly since that time, such as the integrity of the Central Record, considerations in relation to proportionality and use of the urgency procedures. This Force was the subject of a visit by the IPC in January 2020.

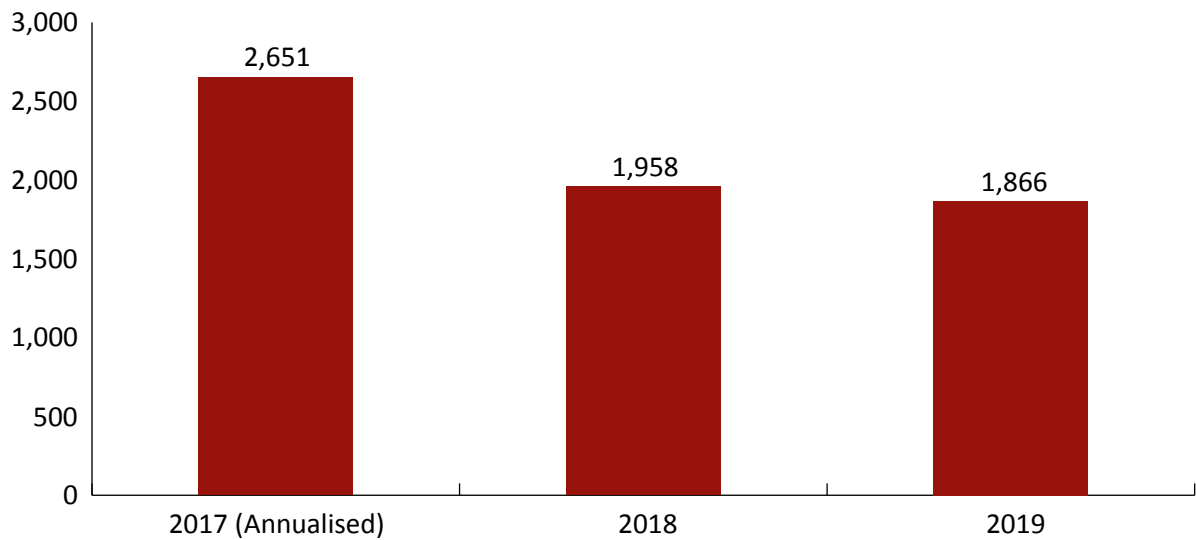
Findings

- 12.3 The level of compliance at the forces we have visited has generally been high, although we continue to make recommendations in relation to record keeping. As discussed below, the differences in the detail of what is required of applicants and Authorising Officers (AOs) can at times be confusing and we believe would benefit from being more consistent. We have made this recommendation to the Home Office, which is responsible for setting policy and guidance across the range of powers. Inevitably, changes in process and the introduction of new authorisation structures leads to different interpretation and can cause some confusion as forces work to comply with the new guidelines; we have seen this play out in terms of targeted equipment interference (TEI) documentation. However, we have noted that the level of engagement with the new processes, available training and discussions about developing consistent policy has been good.
- 12.4 Within many smaller forces the financial and manpower reductions over recent years have meant that whilst there may be the desire to use covert powers in investigations, they are often not pursued or have been curtailed, as the necessary resources are simply not available. Although we were not able to inspect some of the smaller forces in 2018, we did not find in our 2019 inspections that there was an adverse impact on compliance from the cutbacks. In fact, in 2019 there has been an increase in the number of inspections concluding with no formal recommendations.

- 12.5 We have identified training, particularly for officers of the Covert Authorities Bureau (CAB), as a point of vulnerability. Training remains paramount to ensure compliance and improving or enhancing the provision should often be the first step in response to recommendations. However, there appears to be little in the way of a training programme to support CAB staff, and across all covert disciplines there appears to be a shortage of national training courses available. Through our inspections, and from discussions with individual officers, we have found that continuous professional development of all staff is key to ensuring compliance. We hope to see a focus on training at a national level as the need to support transition of the Investigatory Powers Act 2016 (IPA) eases.
- 12.6 In general, we found that the LEAs are making good use of interception tactics across a range of operational requirements and were becoming more ambitious in their use of thematic warrants to disrupt firearms-enabled criminality. Our oversight of thematic warrants has shown that they are being used well, and internal documentation is of a good standard. Use of interception in general has adhered to the Code of Practice (CoP) and the intercepting agencies have made improvements to their processes to accommodate the requirements of the IPA.
- 12.7 Turning to communications data (CD), overall the transition to the Office of Communications Data Authorisations (OCDA) and the IPA has been successful, with the standard of written consideration in authorisations being granted by OCDA on par, and in many cases, better than that seen previously in LEAs. Of course, the process now provides the public additional confidence that applications to acquire CD are considered independently. LEAs retain the power to grant authorisations in urgent circumstances involving threats to life, or where an opportunity to seize critical evidence or make an arrest for serious crime could be lost. Whilst we have, and will continue to focus on, urgent applications, we have found no instances where the use of the urgency provisions has been unjustified.

Covert Human Intelligence Sources (CHIS)

- 12.8 The acquisition of intelligence by CHIS is a core function of LEAs. The term “CHIS” encompasses both members of the public who provide intelligence to the LEA and “relevant sources”, which is the statutory term used to describe staff from a designated LEA that are trained to act as undercover operatives and are subject to an enhanced authorisation and oversight regime. For clarity the former category will be referred to simply as CHIS and the latter as “undercover operatives”.

Figure 2: CHIS authorisations, 2017 – 2019

12.9 There are numerous examples of where CHIS intelligence and undercover operative activity has been instrumental in preventing and detecting crime.

Example 1: Use of CHIS intelligence

A group of burglars were committing a series of offences involving violent confrontation of victims; a CHIS identified the group and this intelligence was passed to the force concerned, allowing investigators to gather the evidence needed to arrest and prosecute the offenders.

Example 2: Use of CHIS intelligence

A CHIS reported on a person who was supplying firearms to criminals. This allowed a proactive operation to be mounted and successfully disrupted the supply of firearms.

Example 3: Use of CHIS intelligence

Undercover operatives, deployed online at sites where paedophiles exchange information and images, were able to identify numerous persons, including several who at the time had access to children.

Example 4: Use of CHIS intelligence

Undercover operatives ‘befriended’ a person suspected of being an Islamic extremist and were able to gather evidence of a terrorist attack being planned by this person and arrest him.

12.10 The vast majority of LEAs have staff dedicated to the management of CHIS and governance of the structures and processes implemented for this purpose. CHIS are typically managed by Dedicated Source Handling Units (or units with similar names), with officers designated as “handlers” and supervisors designated as “controllers”. A senior officer will be appointed as the Authorising Officer (AO, Superintendent or equivalent). There will also often be staff

in the CAB that will oversee compliance with the Regulation of Investigatory Powers Act 2000 (RIPA)²⁷ and quality assure submissions to the AO.

- 12.11 Historically, we have been concerned about the length of time it has taken to assess the suitability of a potential CHIS before granting an authorisation, whilst still accepting intelligence from the source. This is known as 'status drift' and remains an aspect of concern, with occasional cases taking too long before authorisation is sought and granted. This is normally where the LEA in question is seeking to ensure that the source is able to provide intelligence that meets their requirement and to comply with handling instructions, and that the risk (to the CHIS and the LEA) is acceptable.
- 12.12 Managing CHIS cases is necessarily one of the most bureaucratic forms of covert activity in order to create a comprehensive record of the relationship between the CHIS and the LEA, the acquisition and management of intelligence, and the risk assessment. Increasingly we find that there is some unnecessary repetition of details in different records, or most frequently at reviews of cases, where there is a failure to focus on activity that has taken place during the period under review. Instead details from initial applications are restated. The danger with this is that an important fact may not be picked up by a reader as it is buried amongst the extraneous detail.
- 12.13 A significant CHIS error was reported by HMRC in 2019 (see paragraphs 18.3 to 18.4). In brief, HMRC was applying an outdated policy relating to their interaction with witnesses who assisted in a large number of investigations. This meant that the person assisting HMRC met the criteria for authorisation as a CHIS but was not so authorised. A full review was conducted by HMRC and they briefed us on this at our inspection. We conducted a follow-up inspection six months later to ensure that all the necessary remedial action was being taken. We found that a thorough programme of training, re-education and policy changes had been implemented. We recognise that HMRC faces some cultural challenges in embedding the training and education and we will monitor progress at future inspections.

Juvenile CHIS

- 12.14 In the very rare instances when a juvenile is authorised as a CHIS, we conduct a close examination of the case. We examine every such case at inspection and focus on the safety and welfare of the juvenile and check that the use and tasking (conduct) is not endangering the CHIS or leading the juvenile to associate with criminals and environments that they would not otherwise encounter.

Case study: juvenile covert human intelligence source (CHIS)

In one such case, a juvenile was carrying out activity on behalf of a "county line" drug supply group. The juvenile owed money to the group and approached the police wishing to provide information. A referral under the Modern Slavery Act was made by the police and a care plan was drawn up with Children's Services, including relocating the juvenile and finding them a training course. Once this had been done, as an authorised CHIS, the juvenile was able to provide intelligence to the police regarding the 'county line' crime group.

- 12.15 In June 2019, we met a member of the Children's Commissioner's Policy Team to discuss our oversight of this especially sensitive technique, and we are in discussions with the

27 The Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) regulates the use of surveillance and CHIS in Scotland.

Home Office with a view to expanding the guidance in the CHIS CoP in relation to the safeguarding considerations of juvenile CHIS.

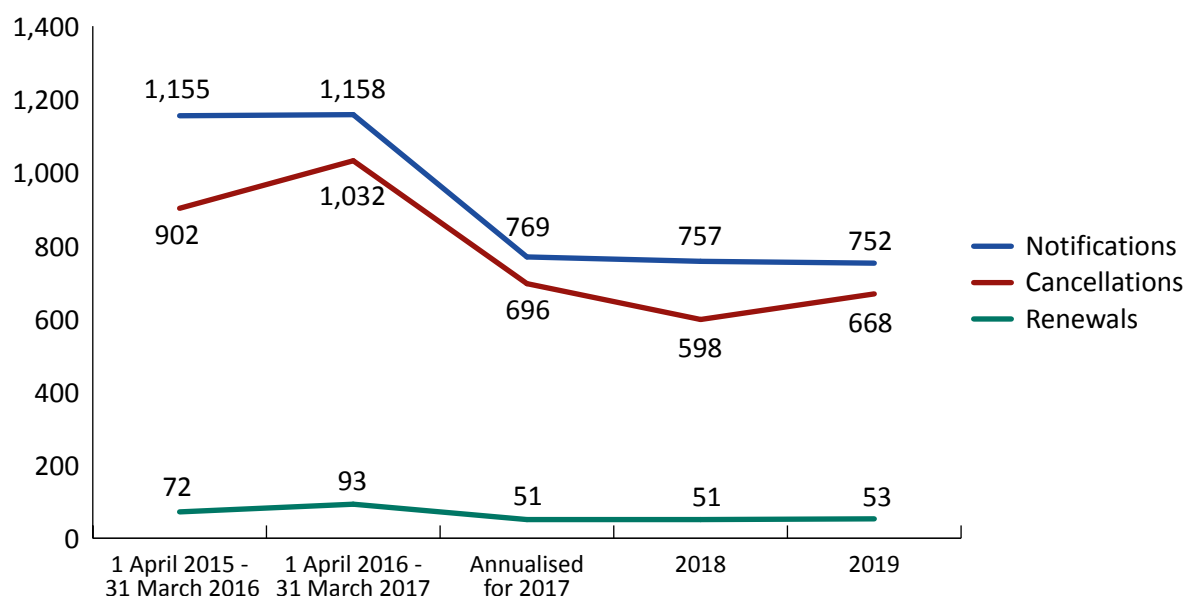
Participation in Criminality

12.16 The use of any CHIS participating in criminality, with the approval of an authorising officer, is also closely scrutinised during our inspections. This, again, is a tactic used very infrequently. It invariably occurs where a CHIS reports an offence that is already being planned or underway and use of the CHIS in a minor role allows the LEA to frustrate, prevent or detect the offenders. Details of the recent Investigatory Powers Tribunal (IPT) case on the lawfulness of the practice of MI5 authorising agents to participate in crime are set out in paragraph 8.10. Although the majority judgment of the IPT held there was a power for MI5 to authorise CHIS to participate in crime, the case highlights the absence of a clear legal framework governing participation in crime. Although the policy response to any judgment is for the Government, we have been involved in discussions with the Home Office about the possible outcomes of the IPT case (which is now pending consideration by the Court of Appeal) and whether enhanced or additional oversight may need to be introduced as a result (see also Legal and Policy, chapter 2).

Relevant sources

12.17 The enhanced authorisation and oversight regime in relation to relevant sources, also known as undercover officers, came about as a result of concern regarding how this form of covert activity was being managed, following several revelations regarding historic cases and a number of police internal investigations.

Figure 3: Relevant source notifications, renewals and cancellations, 2015 to 2019



12.18 We have found that the issue highlighted below in relation to long-term authorisations is particularly prevalent with online undercover operatives. These can often require a law enforcement presence online in relation to crimes such as child sexual exploitation and abuse, terrorism and extremism, for several years. It is also true to say that interaction online with persons who are not committing offences is often fleeting and is a more nebulous relationship than when conducted in the 'real world'. The enhanced regime

for undercover operatives was introduced largely because of the need to have better governance regarding the relationships that were formed during face-to-face deployments and we therefore think it is important that the guidance in the CoP on this issue is clear and followed appropriately. In our view, there should be a presumption towards renewal in these longer running cases, and we have provided the Home Office with a suggested revision to the CoP for their consideration.

- 12.19 We have found that there is a lack of consistency in the approach taken by different forces in relation to long-term operations. We are concerned that in some cases authorisations may repeatedly be cancelled just prior to the twelve-month point rather than being renewed in the longer term. We raised any such cases for discussion at inspection and are consulting with the Home Office to address this area of guidance in the CoP.

Long-term undercover operations

We have identified that the current guidance in relation to long-term undercover operations is causing some confusion and differences in approach across law enforcement agencies. This relates to situations where the operative(s) has been deployed for a cumulative period of twelve months. The authorising officer must decide whether to renew the existing authorisation, or to cancel the authorisation and grant a new one. The former would entail seeking authorisation from a Chief Constable (or equivalent) and the prior approval of a Judicial Commissioner; the latter would revert to an authorisation by an Assistant Chief Constable.

The revised covert human intelligence sources (CHIS) Code of Practice (CoP) gives some guidance as to the factors to be considered when deciding whether the relevant source is authorised as part of the 'same investigation or operation' but the guidance is not explicit enough to allow it to be applied consistently by all forces conducting undercover operations.

- 12.20 We also noted that there is a lack of consistency with the supporting documentation in relation to the briefing, debriefing and record of contact and management of undercover operatives. RIPA and associated provisions are not prescriptive on format, but there is a marked inconsistency in the nature of records that we see during inspections. We also found that there is a good deal of unnecessary repetition in these records. We hope to see an improvement in this area over the coming year.

Surveillance and property interference

- 12.21 As expected, due to the introduction of the IPA, which became effective for law enforcement on 5 December 2018, the number of property interference applications has substantially reduced and been replaced by applications for equipment interference (EI).

Figure 4: Number of intrusive surveillance authorisations and number of directed surveillance authorisations, 2017 to 2019

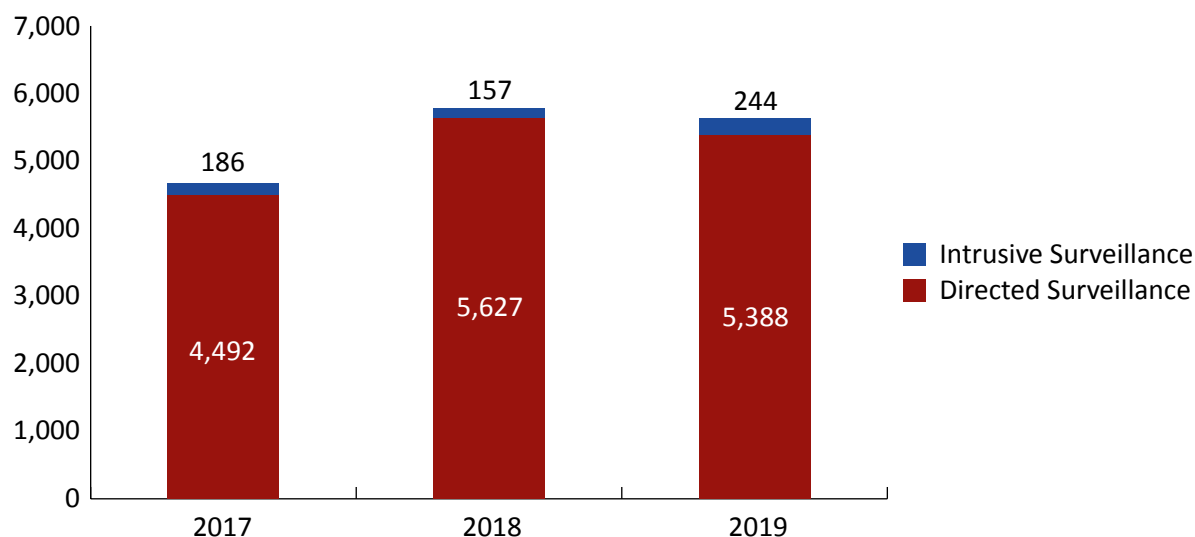
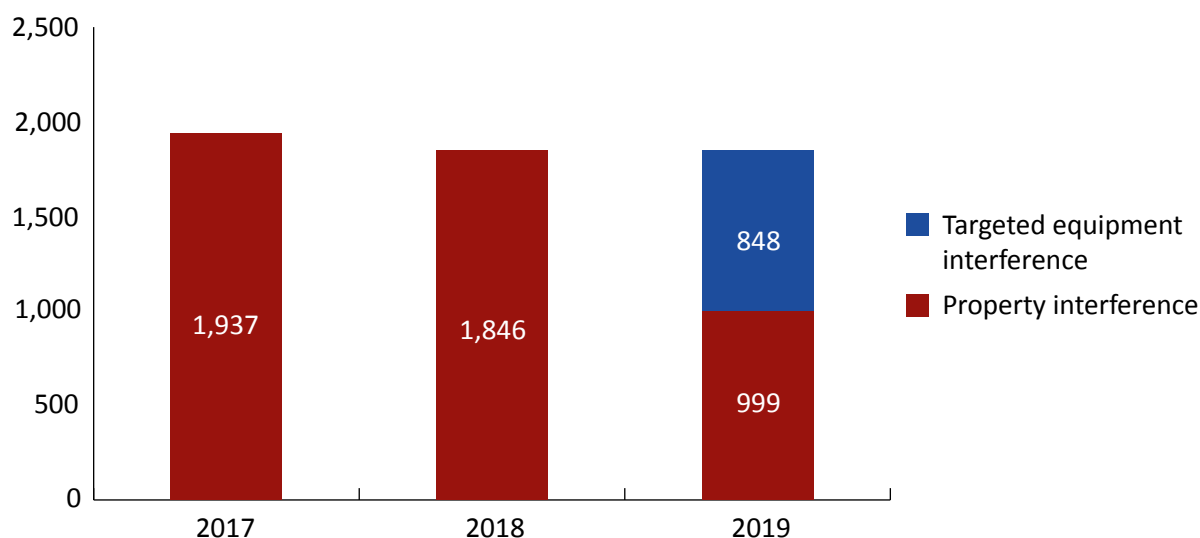


Figure 5: Number of property interference authorisations and targeted equipment interference, 2017 to 2019



12.22 Although standards do vary across law enforcement, we have found the quality and consistency of personnel to be central to a strong compliance culture. Generally, those forces with high standards of compliance with the legislation are those who have excellent oversight by their Senior Responsible Officer (SRO). The SRO should take the strategic lead in respect of all covert activity, have a good relationship with the CAB, utilise professional applicants (where resources permit) and employ Operational Security Officers (OpSy) who have the ability and experience to carry out proactive auditing of compliance and structured reviews of covert operations. We continue to encourage forces to prioritise this role, whilst acknowledging this is a staffing matter for chief officers. Within each LEA, the CAB provides a process of oversight and, in most, a quality assurance function prior to authorisation. As with previous years we found that a high staff turnover reduces the quality of authorisations. This is also the case for frequent changes in the AO.

- 12.23 Some recurring themes, in both formal recommendations or point-of-learning observations, appear throughout inspections in 2019 for both surveillance and property interference. Most prevalent was the consideration of proportionality and associated collateral intrusion; we felt that in some cases the records did not fully address the material required for the AO to make an informed decision in granting the authorisation.²⁸ In these cases, the proportionality argument was usually templated or generic, with most authorising a broad range of tactics without due consideration for each. In direct contrast, a few directed surveillance authorisations were found to be so tightly drawn that errors had occurred. A certain degree of flexibility in the scope of the authorisation should allow authorising officers sufficient oversight while leaving room for trained surveillance officers to work effectively during dynamic operations. We also found issues with review documentation at some forces; reviews often repeated the original intelligence case and did not address the ongoing necessity and proportionality of the tactics requested as identified in previous IPCO reporting. This information is essential for the AO to determine whether it is necessary to continue the operation, irrespective of whether it had been necessary to initiate it in the first place.
- 12.24 There were several forces where the processes for urgent applications for both surveillance and property interference fell below the standards expected, which was contrary to our findings from the previous year. Usually this was due either to a breakdown in the recording process between applicant and authorising officer, or to the urgency criteria not being met or stipulated. We expect to see a significant improvement in this area at these forces in 2020; it is essential that records clearly set out why the urgency provisions are being used and how the relevant case meets the threshold for urgency. In urgent cases, records may be informal, and will often be documented outside of the usual workflow system or application template, but they must still be thorough. We were impressed by the records we examined at one force, which had excellent documentation clearly demonstrating the requirement for applying for authorisations during dynamic deployments.
- 12.25 A feasibility study providing detailed explanation of the proposed technical covert activity was omitted by a number of forces when submitting applications to the AO. The AO should fully understand the capabilities of any equipment being deployed when authorising such activity.
- 12.26 There has been an exponential growth of online activity by LEAs, particularly in relation to open source and social media. There is good evidence of a robust approach to the management of this tactic in some force areas. Yet, there is a risk of status drift into directed surveillance in those forces and regional units where there is no overarching method of identifying all of the product captured. We will focus on this area at future inspections to ensure that online surveillance is properly identified and authorised, and that material is properly handled.
- 12.27 As in previous reports, we continue to see applications in some forces that are overly lengthy and we will continue to make recommendations or observations in this area. We have also found this issue in relation to the approving officer comments, normally the force AO, on applications destined for authorisation by the Senior AO. There is no statutory requirement for this in property interference and intrusive surveillance applications and any comments made should only add issues of real value to support the application.

28 The Codes of Practice for Surveillance and Property Interference Chapter 4 paragraph 4.7 and paragraphs 4.11 to 4.13 fully explain the rationale that the authorising officer needs to consider before granting an authorisation.

- 12.28 We generally found that forces were cancelling authorisations when they were no longer necessary, and we saw an increase in the number of verbal cancellations being given with associated paperwork completed and submitted in a timely manner thereafter. In a small number of forces, there was a delay when submitting the written paperwork. The majority did not include any instruction by the AO as to who was responsible for the retention, review or handling of any product obtained.²⁹ We identified one notable exception, where there was an excellent commentary provided in this area. As noted, we intend to conduct an overarching review of data handling models over the next two years and would expect to see improvements as a result (see chapter 7).
- 12.29 We have found that the review of applications and notifications by Judicial Commissioners (JCs) allows for the identification of minor issues which we can raise with the originating Forces in a process of continuous improvement.
- 12.30 Whilst the majority of law enforcement agencies use a variety of IT systems to maintain records of applications and authorisations for surveillance, there are still some who continue to use hard copy documents. We believe that IT systems ensure better oversight and lessen the risk that documents could be illicitly amended at a later date. Where hard copy records do exist there needs to be a totally transparent and auditable process to ensure integrity of the documentation.

Legal professional privilege (LPP) material

- 12.31 There have been several cases where LPP material has been obtained and we have a high level of confidence that this sensitive material was handled appropriately. However, we found limited evidence that the likelihood, and necessity, of obtaining LPP was well considered. It is usually unlikely that LPP or confidential material will be obtained, but we have found an overreliance on this generality. Some forces have failed to document specific considerations of cases where LPP could plausibly be obtained, for example when a subject is being released from custody for questioning pending further investigation.

Targeted equipment interference (TEI)

- 12.32 The IPA introduced the requirement for LEAs to obtain warrants for conducting TEI in order to obtain communications, private information or equipment data where to do so would constitute an offence under the Computer Misuse Act 1990. This restricted LEAs' ability to use the pre-existing regime of seeking authorisation for property interference under Part III of the Police Act 1997 for such activity. TEI covers interference with any equipment producing electromagnetic, acoustic or other emissions; in more simple terms, this means desktop computers, laptops, tablets, smart phones, other internet-enabled or networked devices and any other devices capable of being used in connection with such equipment. Interference with equipment was not new to law enforcement, although the IPA warrant authorisation process and associated documentation was entirely new.
- 12.33 Prior to the implementation date for LEAs on 5 December 2018, they undertook a national programme of training delivered by the Home Office and the National Police Chiefs Council (NPCC). This ranged from formal online training modules for operational officers to staff awareness and familiarisation sessions delivered at a local level. In most cases, the training

29 Chapter 9 paragraphs 9.1-9.6 of the 2018 Covert Surveillance and Property Interference Code of Practice set out requirements for handling and safeguarding data obtained under surveillance and property interference authorisations.

focused on a general awareness of the changes rather than working through specific challenges of TEI provisions. National coordinators also delivered awareness briefings to chief officers. These focused on what was classified as equipment interference and how a typical deployment would unfold, rather than on a chief officer's additional obligations under the IPA and the TEI CoP.

- 12.34 As the IPA introduces new processes and practices, there are inevitably areas where there are divergent views on what is necessary to ensure compliance. During our inspections, we have seen the use of standard wording contained within a pre-prepared warrant instrument to comply with the requirements of paragraph 5.47³⁰ of the TEI CoP, which are then endorsed by the AO upon issue. Whilst this may meet the legal requirement, we have seen a small proportion of Senior AOs providing additional written considerations of the statutory requirements on the warrant and, in each case reviewed, we have found these to be valuable and well documented. We would encourage this practice, which accords with the approach taken by Senior AOs for authorisations for such tactics as property interference, intrusive surveillance and the use of undercover officers.
- 12.35 TEI applications have the potential to be complex, describing technically complicated and potentially novel actions. This poses a challenge to the authorities applying for warrants because they are required accurately and succinctly to describe the planned operation, as well as the proportionality and collateral intrusion considerations of technically complex operations in a format which is still often unfamiliar. However, most applications we have seen during 2019, both through judicial scrutiny and at inspection, have been for established tactics frequently used under the previous legislation. Applicants therefore have a clear understanding of the scope and impact of their work. With technological advances being made every day, we expect that this challenge will continue to be posed to the authorities we oversee, but we expect to see a consistently high standard of documentation as the process itself becomes more familiar.
- 12.36 Between January and May 2019, we conducted a series of inspections across law enforcement to address potential issues in relation to their use of TEI. Our objective was to reassure the JCs about how the majority of approved TEI warrants were being used; and to inform and develop the future inspection regime for TEI. It was evident to our Inspectors that, across the board, the knowledge and awareness of the safeguard requirements for the handling and retention of TEI material, as set out in the 2018 CoP, was not as it should be. Authorities informed us that they found the safeguarding guidelines unclear. This has been mirrored through our experience via judicial consideration, which has overseen more than 800 authorisations over 12 months. Compliance with the safeguard provisions has been identified as a vulnerability across most LEAs and will therefore be a key focus of our inspections, and specifically our data assurance programme (detailed at chapter 7) throughout 2020.

30 This sets out the tests that must be met before the person responsible may issue a warrant.

Streamlining documentation

Discussions with law enforcement agencies highlighted that the separate administrative processes now in place for targeted equipment interference (TEI), alongside under-cover policing, property interference, and intrusive surveillance authorisations, would benefit from being streamlined. In each case, the process has been differently designed to address the same principles of necessity, proportionality and minimising intrusion. We agree with the view of many police forces that a more consistent administration process would enable both the Authorising Officers and our Inspectors to conduct oversight with greater effect. We expect that this will be considered by the Home Office when they review the success and continued adequacy of the Investigatory Powers Act 2016, although we understand that aligning divergent and established processes could, in reality, be a greater challenge than the benefits that would likely be realised.

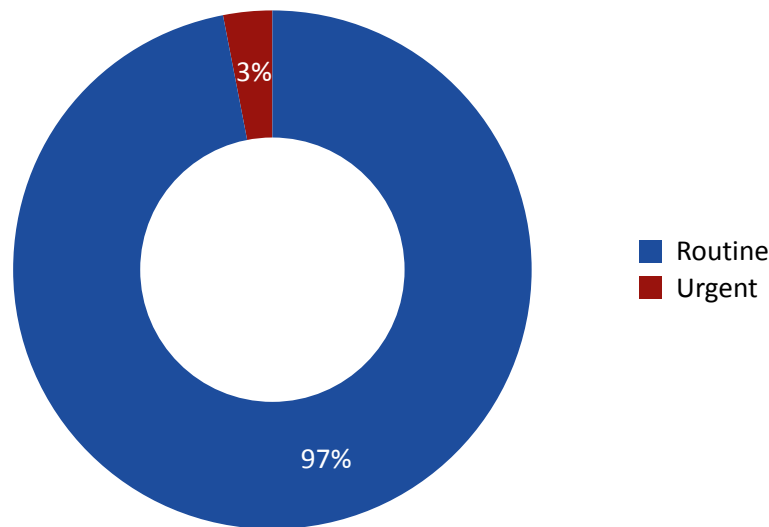
- 12.37 Our oversight has demonstrated that the standard of TEI authorisations has been generally good with some minor 'teething' problems seen during the first few months of implementation. These are associated more with the administration of the new IPA process, rather than issues of legal compliance or the necessity and proportionality of the activity. It is worth noting that we made no formal recommendations in relation to TEI during this short period. We raised a number of observational learning points on the use of templated or generic phraseology seen within some applications, and the need for more bespoke explanations in line with the requirements set out in Chapter 4 of the TEI CoP.
- 12.38 During our inspections and discussions with applicants, as noted in chapter 2, we identified that a general lack of understanding prevailed across LEAs as to what constitutes a thematic or non-thematic warrant, the use of a general descriptor (where it has not been possible to name all the individuals covered by the warrant) and the correct process to follow for modifications. To address this, we have held discussions with law enforcement representatives nationally to improve understanding of these issues and assist them to develop revised guidance and training material for applicants and senior authorising officers.

Targeted Interception (TI)

- 12.39 The use of modifications to amend existing warrants has been a primary focus of our interception inspections. Both major and minor modifications are used to add or remove people and factors to warrants. Minor modifications are authorised within the agency and can be used to either add/remove a factor or remove a subject. The internal authorisation process for minor modifications is a new concept and our focus has been on ensuring that any additional factors added are within the scope of the original warrant application. We will also check to ensure that as soon as a factor is deemed no longer relevant, immediate steps are taken to suspend the interception and a minor modification is submitted to cancel. The minor modifications we examined on our inspections provide full and thorough records of the required interception, clearly set out how the new subject or device is relevant to the warrant and address attribution and collateral intrusion associated with that factor. LEAs have in this year had a small limited use of "thematic" warrants so by far the majority of minor modifications done relate to factors added and removed from "non-thematic" warrants.
- 12.40 LEAs need rapidly to respond to threat-to-life situations and interception coverage can be a useful tactic in protecting the public and saving lives. We examine all urgent oral warrants and scrutinise any internal logs and notebooks which make up the out-of-hours

documentation. These should detail the time and date of liaison with the warrant granting department (WGD) to seek approval from the Secretary of State to effect an intercept. We have found that these records are well kept.

Figure 6: Proportion of urgent and routine applications for targeted interception, 2019



- 12.41 Collateral intrusion can change in the lifetime of a warrant and we identified some room for improvement in some applications and modifications in the way assessment was being made in the potential for collateral intrusion. Specifically, this related to the potential for increased interference with privacy depending on the type of activity being requested. We addressed this by taking part in a workshop with applicants and supervisors and we had input from our own legal team. We are aware of improvement since this workshop and will monitor into next year.
- 12.42 The renewals that we examined documented a good summary of the intelligence value of the interception product obtained to date and outlined why continuance was sought. Any modifications requested after those renewals clearly set out the reasons for any additions or deletions. Cancellations that we saw were promptly submitted when subjects were arrested, disrupted, or when continued interception was no longer considered either necessary or proportionate.
- 12.43 We have access to the systems used by LEAs to manage targeted interception. We checked random selected samples of warrants that have been renewed by searching these systems to ensure they are still necessary and proportionate. We cross referenced this with relevant modifications. The samples we checked were to a high standard and we are satisfied that in those samples, warrants are being cancelled if no longer necessary or proportionate.

Sensitive professions

- 12.44 Our inspection regime focuses on how each intercepting agency handles any confidential and legally privileged information collected and the arrangements for its storage or deletion. Before each interception inspection, we review a list of all warrants where the subject holds a sensitive profession and where sensitive material has been obtained. This includes all legally privileged material, confidential personal information, confidential journalistic material or communication with a spiritual counsellor which has been intercepted and retained.

- 12.45 We review overarching policies and consider the level of understanding and adherence to those policies within the agency to be essential to their adequacy. We therefore test internal policies and procedures by asking staff who transcribe the material directly how they manage and process it. We also conduct searches on LEA internal IT systems to confirm that any confidential material has been deleted when it should have been, or if retained that the appropriate authorisations are in place. As a final step, we check that, if LPP or confidential material has been collected, this fact has been mentioned and given due consideration in any renewal application. We were pleased to note that across the board there was very good compliance with the handling of LPP and confidential material. Since the introduction of the IPA, the intercepting LEAs have introduced more quality control and resources to ensure that their safeguards are robust. This was clear through our interviews with staff.

Communications data (CD)

- 12.46 2019 brought the most significant change to how LEAs acquire communication data (CD) since legislation was first introduced under RIPA in 2000. In response to the European Court of Justice ruling,³¹ the IPA was amended to implement two major changes: the introduction of a serious crime threshold³² and independent authorisation of all routine applications to acquire CD by OCDA (see chapter 5). Our inspections have overseen the adequacy of this transition and how well forces have met the different requirements of RIPA and the IPA pre and post-transition.
- 12.47 The fundamental requirements of acquiring CD have not changed and the main focus of our inspections has been to ensure that applications and authorisations are necessary for one of the relevant statutory purposes, proportionate in what the application seeks to achieve, and that due regard has been paid to the risk of obtaining any unrelated private information (collateral intrusion).
- 12.48 Overall, the general standard of compliance across LEAs is high, due in no small part to those LEA staff members who act as Single Points of Contact (SPoCs) and the integral role they play to maintain compliance and manage key areas of risk. We have found that the SPoC role provides both challenge and quality control for applications. SPoCs we have interviewed demonstrated a good level of knowledge of the technology and tactics available to the force, which allows them to advise and challenge Senior Investigating Officers (SIOs) on the most appropriate method of applying CD tactics. This is essential to ensuring compliance with necessity and proportionality principles, whilst safeguarding the privacy of the public. We have been pleased to note a decrease in the number of reportable errors, which we believe has resulted from the professionalisation of the SPoC role as well as the introduction of auto-acquisition of CD³³ and the introduction of the National Errors Reduction Strategy.

31 Joined cases C-203/15 and C-698/15

32 This was implemented at the end of 2018, see IPCO's 2018 Annual Report paragraph 2.40.

33 Once authorised the data can automatically be acquired through the workflow system without the need for the request to be manually re-typed into a separate portal.

Definition: reportable error

A reportable error occurs when incorrect communications data is acquired; such as a disclosure to an agency that could infringe on the rights of an individual unconnected to an operation or investigation. Reportable errors should be recorded within five working days of their discovery. The error report explains how the mistake occurred, indicates whether any unintended collateral intrusion has taken place, details and confirms the destruction of data and provides an indication of steps taken to ensure similar errors are not replicated. When a report is made, the appropriate Senior Responsible Officer (SRO) must be sighted on the error to enable, if necessary, any strategic changes to policy or procedures.

Data Protection Act 2018 (DPA) vs Investigatory Powers Act 2016 (IPA)

Law enforcement agencies (LEAs), including police forces, can request data from telecommunications operators (TOs), who may disclose the data requested under exemptions in the Data Protection Act 2018. As more LEAs have transitioned to the IPA for communications data (CD), practical application of the legislation has highlighted a grey area where the guidelines need to be reviewed regarding the use of these powers which result in acquisition of CD and the clarification of what constitutes a telecommunications service.

Before the IPA, an LEA could seek certain information from online retailers under the Data Protection Act 1998, for example if they needed data about a stolen credit card used to buy goods online, or to identify the address of a person selling stolen property on a web-based market place. The retailer could release that data under an exemption in the 1998 Act for use in preventing or detecting crime. Often, the data released included elements of CD that were inextricably linked to other account details, even though this data was not necessarily asked for or required.

The Data Retention and Investigatory Powers Act 2014 expanded the definition of 'telecommunications operator' to include companies who provide internet-based services, such as webmail and online retail. When the IPA came in, a further major change was the creation of an offence in section 11 for knowingly or recklessly acquiring CD without lawful authority. Although it provides an important safeguard, this offence, when combined with the ambiguity and complexity of the definition of CD, poses significant challenges for public authorities.

For example, most online retailers do not understand themselves to be offering a telecommunications service and do not therefore recognise the requirement to respond to a CD notice under the IPA – instead, they often insist upon the use of the DPA. The outcome is that for what, in most cases, are relatively straightforward LEA requests for basic user information to assist in the detection of a crime, an authorisation for the CD element is required under the IPA and a request under the DPA for other personal data. It also means that a CD authorisation or notice may be sought out of an (understandable) abundance of caution (given the potential for criminal liability), even when the data is unlikely to constitute CD.

Whilst this complies with the guidance in the Code of Practice (CoP) and Home Office advice, it creates what we believe is often an unnecessary process for the applicant, the Office for Communications Data Authorisations (OCDA) and the retailer, and appears to have created additional bureaucracy above and beyond what would have been envisaged by the safeguards introduced under the IPA. We will continue to work with LEAs and the Home Office to resolve this issue in 2020.

Internal investigations and professional standards

- 12.49 Internal corruption investigations, often progressed by siloed Professional Standards Units, are a sensitive area of work in any police force. Many of these units are small and, although they are staffed by experienced officers, they are typically low-volume users of covert tactics compared to other investigative units. We have ongoing concerns with a proportion of applications by Professional Standards Units where some investigations appear to follow an approach, narrowly focused on CD, where very often a large and unnecessary amount of data is sought and retained. At several forces, we recommended that reduced time-scales relevant to the events in question should be specified in applications. We have advised that the available 12 months of data should not be used as a blanket requirement. Our inspections have identified that lower-volume users, such as anti-corruption units, may default to requesting more data than necessary because of a lack of familiarity with the process. We expect to see this practice reducing in response to our observations.
- 12.50 As highlighted in 2018, we noted a failure in many cases to explain adequately the crime being investigated. We saw some improvement in this area after the transition to OCDA authorisation and expect that the completion of transition should have eliminated this issue. The serious crime threshold must be clearly articulated to OCDA authorising officers for the application to be approved. We expect all units to adhere to this requirement and will examine records at smaller units such as professional standards to ensure that this improvement is made in 2020.
- 12.51 CD sought in relation to internal investigations must meet a threshold where there is a reasonable prospect that the Crown Prosecution Service (CPS) would progress charges against the subject if the investigation provided the evidence expected. Applicants should therefore bear in mind the CPS's advice in relation to Misconduct in Public Office. Casework we have inspected has often fallen short of providing a clear statement setting out the nature of the misconduct and has not made reference to those guidelines. This has meant that the severity of the offence is often unclear and we have observed that this should not be the case on any applications. These applications are now considered by OCDA and the Inspectorate has provided specific guidance on this issue to approving individuals.
- 12.52 We have also highlighted the need for the Senior Responsible Officer in each LEA regularly to scrutinise long running or multiple applications to ensure the continuing necessity and proportionality. We would expect to see this in place by our 2020 inspections.

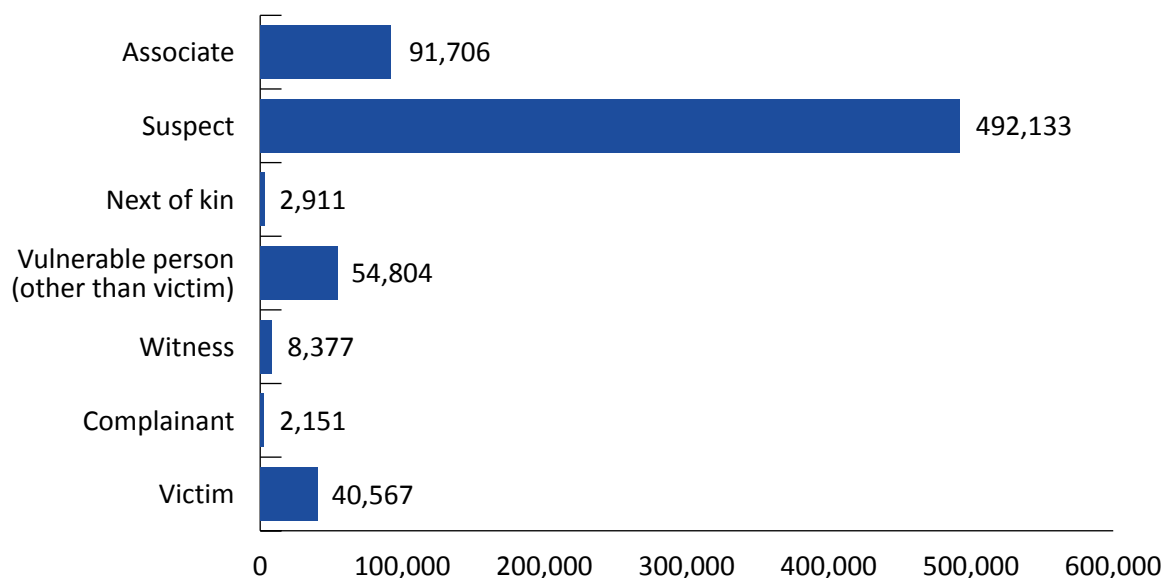
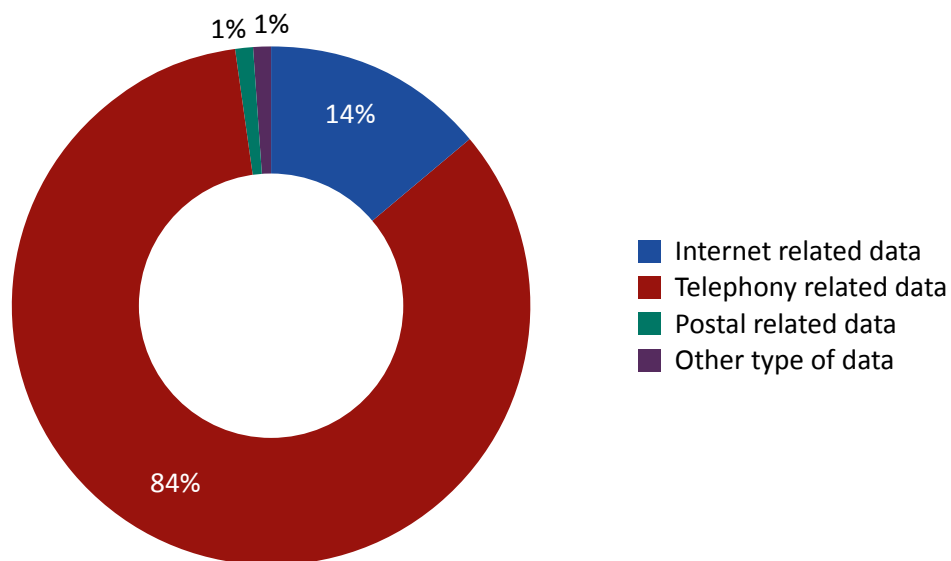
Sensitive professions

- 12.53 In 2018, we reported that the nature of the data in relation to sensitive professions was not always being well considered and that we would like to see a clearer articulation of human rights considerations in relation to these. We have seen some improvement, but concerns remain with some applications that involve sensitive professions and we have observed that the definitions may be applied too narrowly. We continue to encourage SPoCs and applicants to think more widely as to what constitutes a sensitive profession.³⁴ The temptation just to use the examples in the CoP as an exhaustive list can imbue a sense that considerations need only be applied in those specific circumstances and can lead to inconsistencies. In one case, for example, we examined an application relating to an imam which included no additional considerations. On the other hand, however, we have seen examples of good practice, such as where additional considerations were documented for mental health nurses and local councillors.

34 Guidance in relation to sensitive professions is given in the CD Code of Practice paragraphs 8.8 – 8.11.

Freedom of expression

- 12.54 Following on from our work in 2018, we have continued to focus on how well forces set out the applicable crime threshold in their requests. Applicants are required to state which crime is under investigation but, on occasion, we can see some offences broadly and non-specifically described as “harassment offences” or “communications offences”. Clarity in this regard is important for two reasons (i) to ensure that the offence is one which crosses the serious crime threshold if events data is sought, and (ii) to ensure that the public authority is aware of a person’s freedom of expression. This point has been a priority this year; we have focused on the implication of the acquisition of CD in terms of potential interference with the subject’s rights over and above their right to privacy – specifically Article 10 ECHR (freedom of expression).
- 12.55 We identified a small number of cases where the police have investigated those who have sent messages which may upset the local community but, in our view, are a long way short of being grossly offensive. In general, however, we have found that police rarely use their investigatory powers in such a context, and most investigations into malicious communications or harassment are clearly within the criminal threshold relating to domestic violence or clearly threatening behaviour rather than social media disputes between people of differing political, philosophical or religious opinion. We will remain vigilant in this area as we recognise the police are often called upon, and feel pressure to, address non-criminal social issues. We have made recommendations to LEAs that, in order to allow for applications relating to harassment and communications offences to be duly considered by OCDA, they must include an accurate summary of what was said or communicated to help authorising officers determine if the criminal threshold is met.
- 12.56 The need to review data retention and handling is covered elsewhere in this report but we have had initial conversations during inspections in relation to CD retention. These discussions have identified potential vulnerabilities, including the failure of some workflow systems to allow for automated review, retention and disposal processes (RRD) and the practice of individually saving copies of communications data on desktops during investigative work. More details on how we will investigate these issues in 2020 are set out under Data Assurance (see chapter 7).

Figure 7: Communications data items by individual (subject), 2019³⁵**Figure 8: Communications data items by communications type, 2019**

35 Note that the figures for communications data were not consistent throughout the 2018 Report. The figures given in the 2018 Report do not give the same total number for communications requests. This reflects the data we receive from authorities. There is a margin of error on communications data which means that the total number of line items is inconsistent. This reflects differences in how the authorities we oversee collect and collate these statistics. Note that the margin of error is approximately 10%.

Figure 9: Communications data items by data type, 2019

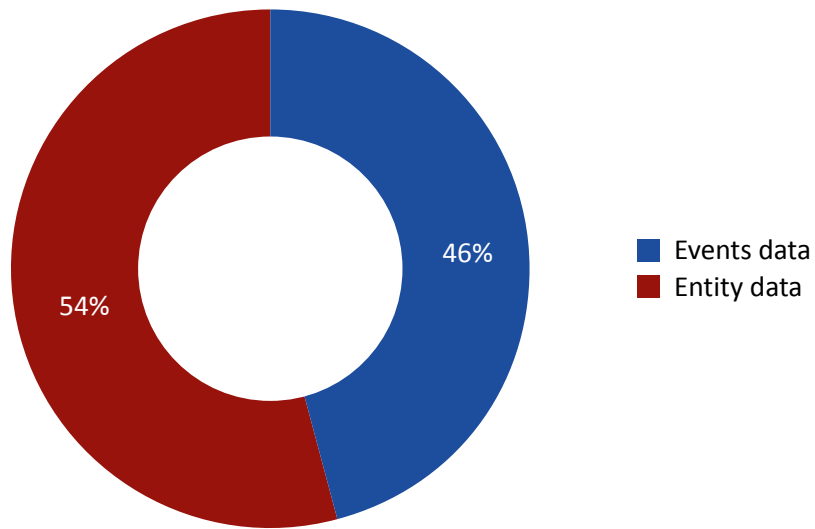
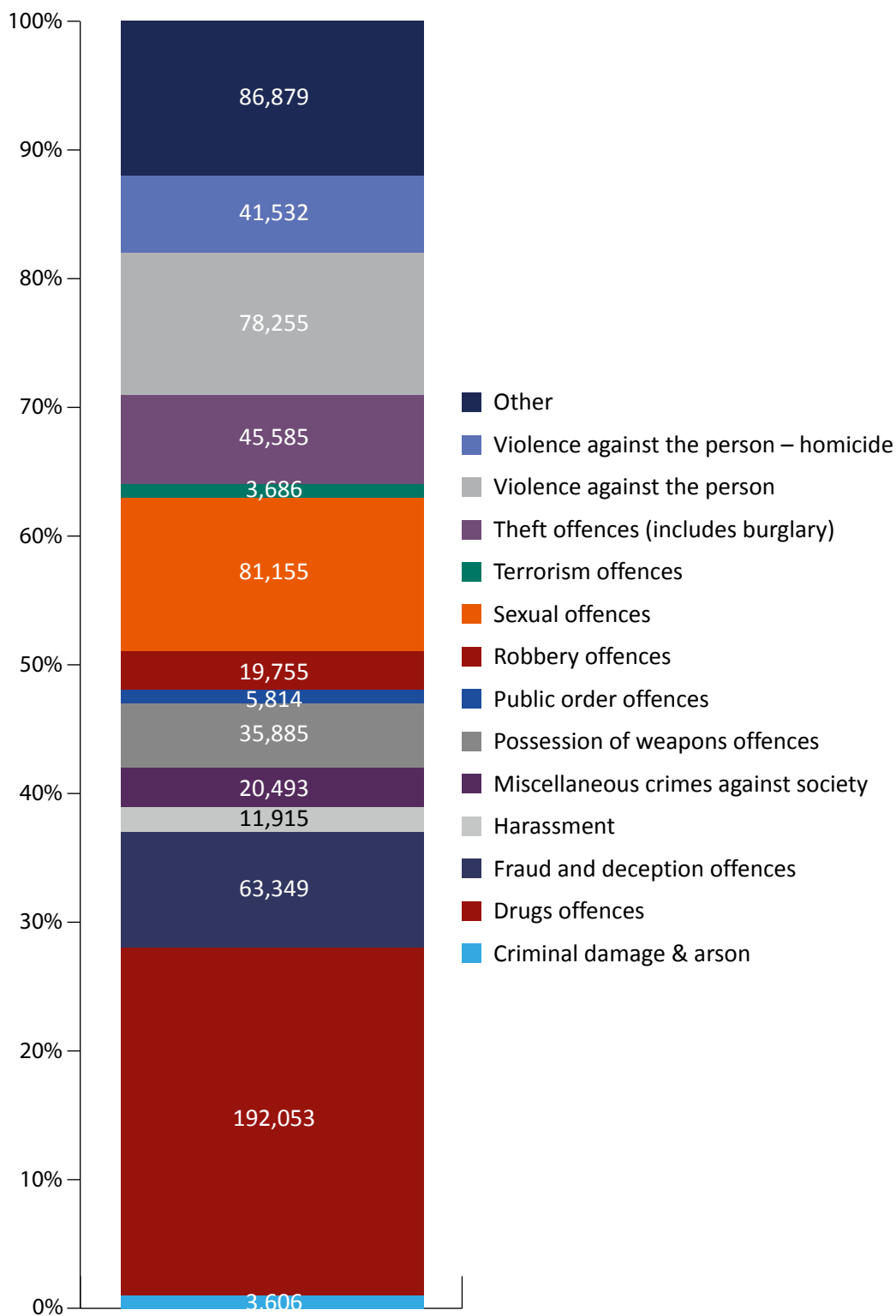


Figure 10: Communications data items by offence, 2019³⁶

36 "Other" might include applications related to corporate and business numbers, or for network service information where it is not possible at the time of application to identify a relevant user, for example seeking data from a cell site, or a public internet service. These categories are allocated by the requesting organisation and not by IPCO.

Data assurance

- 12.57 As detailed in chapter 7, we have initiated a programme of work to investigate the data handling processes across all of the authorities we oversee. As the first stage in our data assurance programme, we required all LEAs to complete a self-assessment of their current processes and identify potential vulnerabilities in their data handling model. At the end of 2019 this programme was in its early stages, but we had identified some potentially serious shortcomings which need to be addressed. It is worth noting that we have no sense that any agency has deliberately mishandled data, but the following themes will help give a focus to our work with LEAs in 2020.
- 12.58 In relation to the IPA, the self-assessments did not highlight any issues with targeted interception material, which is handled on bespoke workflow systems which do not allow the download of information to be stored elsewhere. The self-assessments suggested that there may be some vulnerabilities in the handling of targeted equipment interference material, in particular that data might be shared using emails and stored to personal or shared desktops for analysis. This issue will be investigated thoroughly before we confirm whether there are any errors in handling this data. Our concern here is that email systems are not subject to automatic retention, review and disposal processes. This means people may file emails in folders for future review and then not delete the material in line with the schedule. In most organisations emails automatically back up and are capable of being recovered after deletion, meaning that the material contained in the email is retained on a server longer than is anticipated by the recipient. Similarly, our concern in relation to personal and shared desktops is that, at the end of an operation, officers will not always delete all the material they have stored. It is also possible that if officers can hot desk, then certain systems will back up the data on individual computers. This could mean that if an officer logs into computers A, B and C over a month and, at the end of the operation logs into computer A and deletes the material from his personal desktop, a shadow copy of the material might be retained, and still technically be accessible, on computers B and C despite not showing on his desktop viewer. We will need to investigate the implications of these concerns at each force individually.
- 12.59 Police forces use one of three commercially available workflow systems for handling CD. The self-assessment responses have suggested that one of these systems does not have a disposal capability and a second does not automatically apply review and disposal processes. We are therefore concerned that a substantial proportion of communications data material is not being deleted appropriately. We have also noted that emails are used to obtain material from certain telecommunications operators (TOs). In most cases, we believe that data can be exported from the workflow systems for analysis and saved to personal and shared desktops. We will investigate the extent of this vulnerability with each force we oversee and at a national level given the commonality of the issue.
- 12.60 Property interference and surveillance techniques rely on a range of systems and equipment which are retained and handled within specialist units. It has therefore been difficult to identify trends from the initial returns so we will investigate this issue with operational teams throughout 2020.
- 12.61 LEAs implement exceptionally tight controls around CHIS material because of its sensitivity and the crucial importance of safeguarding CHIS identities. We were therefore not surprised to find that self-assessments detailed the use of workflow systems that are only accessible to a small number of individuals and from which nothing can be downloaded. The retention period of all material relating to a CHIS is typically longer than for other forms of data because it may be necessary to access it for the CHIS's protection, throughout

their lifetime. We will nonetheless investigate whether those retention requirements are properly implemented at each force.

- 12.62 In summary, it is immediately clear that there are a number of vulnerable areas that we need to investigate further. Our investigations need to consider both the technical environments used by officers at each organisation and the way that individual teams are using their data. It is vital that this work is completed to ensure that all data is held and disposed of lawfully, while still ensuring that law enforcement officers are able to conduct operations effectively. We will therefore work with each force to identify and mitigate any risks and vulnerabilities as efficiently as possible. However, the severity of these potential vulnerabilities must not be underestimated. There is the potential that some data may not be held lawfully and this may have serious implications for the continued use of those powers. We will work closely with the Home Office and other relevant bodies to ensure that this matter is fully understood and investigated as this programme continues.

Protected information

- 12.63 Under section 49 of RIPA, specified public bodies may require the disclosure of protected information, which they have lawfully obtained or are likely to obtain lawfully, in an intelligible form or to acquire the means to access the information. The National Technical Assistance Centre (NTAC) is the lead national technical authority for this type of activity and advice must be sought from NTAC before an application can be made to the appropriate authority for permission to exercise these powers. These powers are used infrequently with 139 approvals granted in 2019 and none refused. This is a significant increase over the 66 approvals granted in 2018 and reflects better security awareness by subjects of interest and greater awareness of this capability in the LEA community.

13. Wider public authorities

Overview

- 13.1 Several public authorities, in addition to Law Enforcement Agencies (LEAs) and local councils, have the statutory power to use certain covert tactics. We refer to these authorities as Wider Public Authorities (WPAs) and include a list at Annex A. The nature and extent of these powers differs across the WPAs dependent on their functions. Several, although not all, are empowered to authorise the use of directed surveillance and the acquisition of communications data but the tactics requiring a higher level of authorisation (property interference and intrusive surveillance) are limited to a smaller number of WPAs.³⁷ In relation to the authorisation of covert human intelligence sources (CHIS), many WPAs do have the statutory power but most have chosen not to exercise it, citing (amongst other reasons) a lack of appropriately qualified and trained staff to fulfil the roles of handler³⁸ and controller, or an ability to achieve their objectives by pursuing less intrusive means. However, some WPAs have reported that they are reviewing their policies not to authorise the use and conduct of CHIS in recognition of the changing nature of the criminal enterprises they are encountering, particularly online.
- 13.2 WPAs deploy covert tactics in support of a broad range of investigations which reflect the diverse nature of the investigative and enforcement functions they perform. Principally these are:
- to investigate and prosecute breaches of company and insolvency legislation;
 - investigation of fraudulent benefit claims;
 - tackling environmentally damaging pollution; and
 - the regulation of medicines, medical devices and equipment used in healthcare.

Findings

- 13.3 We found that the generally high standards identified in the 2018 report have been maintained. Those WPAs which exercised their powers on a regular basis attained the highest standards of compliance and often benefited from deploying experienced staff in Covert Authorities Bureaus (CABs) to quality assure the application and authorisation process. A recurring recommendation has been the continuing failure by many Authorising

37 Property interference can only be authorised by the Competition and Markets Authority (CMA), Independent Office for Police Conduct (IOPC), Police Investigations and Review Commissioner, or the Home Office. Intrusive surveillance can only be used by the Competition and Markets Authority (CMA), Independent Office for Police Conduct (IOPC), the Home Office (for customs and immigration matters only) and the Ministry of Justice and Northern Ireland Office (in both the latter cases, for activity in prisons only).

38 A handler has day to day responsibility for dealing with the source on behalf of the public authority and for the source's security and welfare. The controller has general oversight of the use made of the source and is responsible for the management and supervision of the handler.

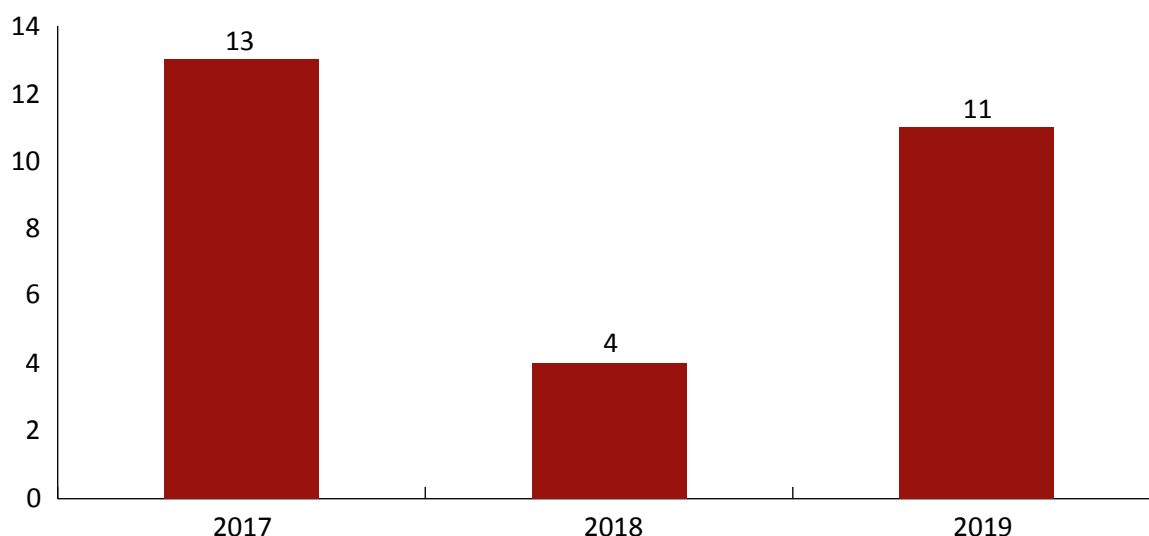
Officers (AOs) within public authorities unambiguously to set out what activity is authorised in order that those conducting the surveillance are clear on what has been sanctioned. We will look closely at this in 2020, because such ambiguity leads to the risk that unauthorised surveillance might be conducted inadvertently.

- 13.4 CHIS powers were used rarely but well by WPAs. Our inspections at most authorities considered whether proper training and processes were in place to ensure that CHIS were not run without appropriate authority and that staff understood the key principles. Even if the powers were not being used, this would ensure that any future CHIS activity would be compliant.

Covert human intelligence sources (CHIS)

- 13.5 We inspected each authorisation for the use of CHIS in 2019. Notable findings from these inspections included one WPA which had good processes in place to deal with potential legally professional privileged (LPP) material and which had followed the requirement to implement a higher level of authorisation in this event. At another inspection, we noted a good level of compliance although only one CHIS case was active. This inspection found a robust and questioning attitude to the management of CHIS coupled with suitable processes in place to support it.
- 13.6 In several WPAs, the power to authorise CHIS has been relinquished, either because there is no requirement or because of a recognition by the authority that the infrastructure, training and knowledge required compliantly to manage CHIS did not outweigh the potential intelligence benefits to be gained.

Figure 11: CHIS authorisations for wider public authorities, 2017 to 2019



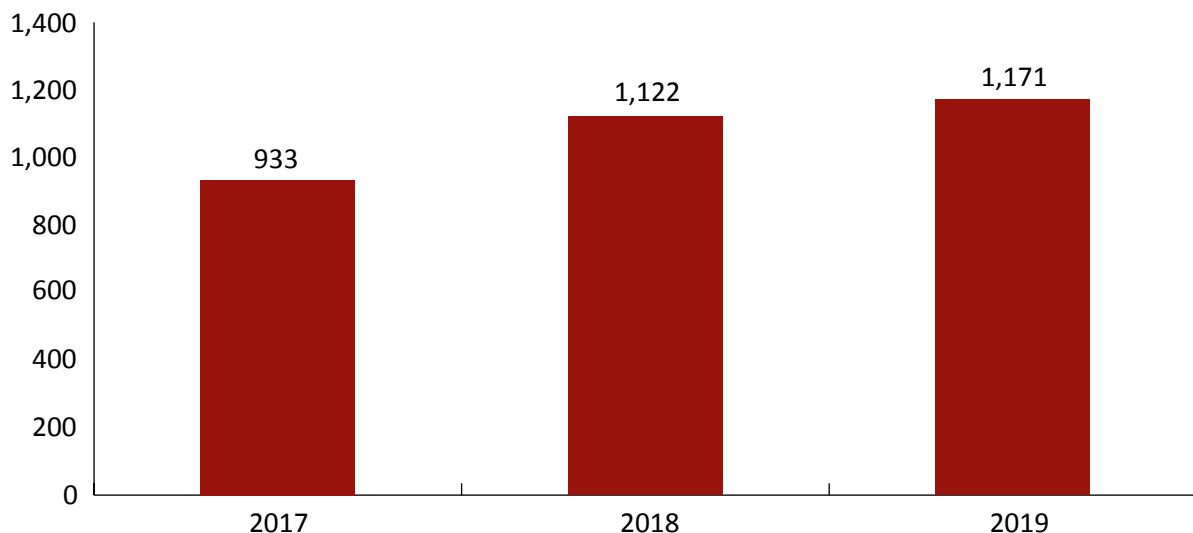
- 13.7 Status drift is the term we use to describe when the forming and maintaining of a relationship with a member of the public who is supplying information, without a CHIS authorisation in place, changes to a relationship where the individual is being tasked to obtain information covertly on behalf of the authority and a CHIS authorisation would be required. We look for occurrences of status drift during all of our inspections, especially of those which have staff in contact with the public and of those that do not have the power to authorise CHIS. We also look for instances where the organisation may be establishing a relationship with an individual who is being questioned or tasked in a way that should be

considered CHIS activity. Previously, we were concerned that some WPAs showed a lack of understanding of when a member of the public or other informant should be considered a CHIS. We test the knowledge of staff, irrespective of the existence of active authorisations, to check that no incidents of 'status drift' have occurred or are likely to occur. In all cases, WPAs need to have clear and unambiguous policies setting out how routine work, such as asking a member of the public to make a 'test purchase' of an unlawful item or conducting an investigation online, can evolve such that it would be appropriate to consider a CHIS authorisation. We commonly encouraged the continued education of staff to ensure that processes and procedures were up to date and that any changes in legislation were reflected within internal policy documents. Additionally, we have reminded several WPAs to consider whether they have a duty of care towards any individual that provides them with information on which they might later act. We inspect records of information obtained from these informants and have advised that these should be well kept, even where there is no CHIS authorisation in place or planned.

Surveillance

13.8 During our inspections, we focus attention on the use of the internet and social media by WPAs. Many WPAs have embraced the considerable opportunities presented by the internet to respond to the emerging threats posed by cyber-enabled and cyber-dependent crime. The Environment Agency, for example, has produced a fourfold increase in the number of directed surveillance authorisations to enable online investigative research to tackle illegal waste disposal. The results of these enquiries have been very impressive, providing significant evidential and intelligence material.

Figure 12: Surveillance authorisations, 2017 to 2019³⁹



13.9 Our inspections have also highlighted the importance of keeping guidance up-to-date, in line with the revised Codes of Practice (CoP) and the legislative changes brought into force by the Investigatory Powers Act 2016 (IPA). The new CoP provides guidance on the use of the internet and social media which, if properly applied, should ensure that such resources are used in a controlled, auditable and well understood manner. However, it is also

³⁹ In addition, the BBC granted 23 authorisations in relation to 328 addresses for the detection of television receivers pursuant to the RIPA (BBC) Order 2001. The 2001 Order treats TV detection as "surveillance not otherwise covered" by RIPA and instead provides a bespoke authorisation process.

essential that WPAs have the necessary training and awareness arrangements in place to provide practical examples and scenarios that users can relate to in their day-to-day roles.

- 13.10 In the spirit of the legislation, WPAs use covert tactics only if available overt means of achieving their objectives have been considered. Our 2018 report highlighted failings by certain WPAs clearly and explicitly to set out the activities that were being authorised. At our 2019 inspections we noted improvements in this area, for example when directed surveillance powers were exercised we found that documented considerations were clearer. However, there is still room for improvement in proportionality considerations, such as setting out which overt tactics had been considered or used without gaining the required information. We have found when reviewing casework that AOs who have a background in law enforcement tended to be more familiar with the human rights principles engaged by the processes under the Regulation of Investigatory Powers Act 2000 (RIPA), and therefore will often attain much higher standards of compliance than their colleagues. We believe that the opportunity for these officers to share their knowledge and act as mentors to their colleagues should be taken to improve the overall standard of applications and authorisations.

Communications data

- 13.11 In 2019, we inspected 13 public authorities, all of which had used their communications data (CD) powers in some capacity during the year.⁴⁰ Compared to the law enforcement agencies (LEAs), these public authorities are generally low-volume users of powers.⁴¹ During our inspections we review a higher than typical proportion of authorisations, addressing the risk that less frequent applicants might not document considerations and apply safeguards to the expected standards. This risk, however, is also limited by the structures in place under the IPA to process CD requests.
- 13.12 The schedules to the IPA set out which authorities can use specific powers and are subject to revision. In 2019, Schedule 4 was commenced with the effect that four additional public authorities became able to obtain CD. These authorities are: Food Standards Agency (FSA); Food Standards Scotland – Scottish Food Crime and Incidents Unit; Department for Communities in Northern Ireland and Department for the Economy in Northern Ireland – Trading Standards. As these public authorities only recently had the power to obtain CD granted or re-granted to them we did not conduct inspections in 2019. In 2020, we will review any applications that these authorities have made as well as the adequacy of their systems and processes for handling and safeguarding that data.
- 13.13 WPAs all apply for CD with independent authorisation via the Office for Communications Data Authorisations (ODCA) (see chapter 5), except in exceptional circumstances e.g. urgent cases. Following transition to the IPA, WPAs can acquire both entity and events data if they fulfil the necessary statutory criteria. For many, this makes data that is more complex and

40 The Competition and Markets Authority (CMA); the Criminal Cases Review Commission (CCRC); the Department for Transport – Air Accident Investigation Branch (AAIB) and the Maritime and Coastguard Agency (MCA); the Department for Work and Pensions (DWP); the Home Office Immigration and Enforcement Directorate (HOIE); the Department of Health and Social Care – Medicines and Healthcare Products Regulatory Agency (MHRA); the Gambling Commission; the Gangmasters and Labour Abuse Authority (GLAA); the Health and Safety Executive (HSE); the Independent Office for Police Conduct (IOPC); the Ministry of Justice – Her Majesty's Prison and Probation Service (HMPPS), and the Serious Fraud Office (SFO).

41 With the exception of the Department of Work and Pensions and the Serious Fraud Office, which conduct investigations using CD on a more frequent basis because of their remit.

more intrusive available to them for the first time. In brief, entity data will identify the user of a device or address, while events data may identify communications (but not their content) made by the device during a given timescale and could identify where the device was when it was being used. For this reason, the request needs carefully to be structured to ensure that only the necessary data is requested and obtained. The increased complexity when applying for and handling events data supports the need for subject matter expertise in both the application and acquisition of data: this role is fulfilled by OCDA and the Single Point of Contact (SPoC).

- 13.14 As at other authorities, the role of the SPoC is vital to ensuring compliance standards are maintained. Dependent on their size and structure, some public authorities have their own staff trained⁴² as accredited SPoC to acquire data from telecommunications operators (TOs), whilst others utilise the centralised services of the National Anti-Fraud Network (NAFN) (see chapter 14). In some cases, we observed that using a single in-house SPoC provided little resilience for the organisation. We advise that a collaboration agreement⁴³ is appropriate to resolve this risk, by giving the authority access to additional accredited SPoCs. We have also recommended at times that the authorities must ensure that the national list of accredited SPoCs is properly updated when individuals move and change roles.
- 13.15 Our inspections of CD generally noted a high standard of compliance. In respect of the application records we sampled, we continue to be satisfied overall that the documentation reflects the complexities of their investigations and justifies the principles of necessity, proportionality and collateral intrusion. We made a small number of recommendations, most of which related to how the organisation was addressing Internet Protocol Address Resolution (IPAR), record keeping when relying on urgent oral provisions and effecting changes within applications. As noted in chapter 18, IPAR is a priority for our oversight because CD applications relating to IPAR have historically resulted in a high proportion of errors. IPAR requests are a new capability for WPAs so our priority has been to ensure that processes implemented at each authority adequately reflect the National Error Reductions Strategy of the National Police Chiefs Council (NPCC).
- 13.16 We made a number of common observations which are intended to encourage greater efficiency and standardisation across the authorities we oversee. For example, in some cases we noted that authorities were using national templates but without the benefit of common workflow systems which are designed to automate certain processes and to eliminate human transposition errors. Similarly, authorities that do not have access to telecom operator (TO) portals, and therefore rely on manual interaction, would benefit in efficiency terms from adopting this methodology.
- 13.17 We understand that low-volume use by a public authority impacts upon any justification to have multiple SPoCs or to support any business case to introduce bespoke workflow systems or access TO portals. In cases where it is not appropriate or proportionate to adopt these measures, we advise that engagement with OCDA will assist with those requests seeking data types new to the public authority and ensure the correct course of conduct is being applied.

42 As set out in the Code of Practice (CoP) paragraph 4.4, the Home Office National Communications Data Service works with public authorities to ensure all accredited SPoCs receive adequate training, run by the College of Policing, and issue accredited SPoC with a unique identifier.

43 Under section 78 of the Act, public authorities may enter into a collaboration agreement which allows one public authority to use a SPoC working for another authority. These provisions are clarified in the CoP paragraphs 8.55-8.58. A written agreement should be in place, and the Home Office must be notified before the agreement is in place.

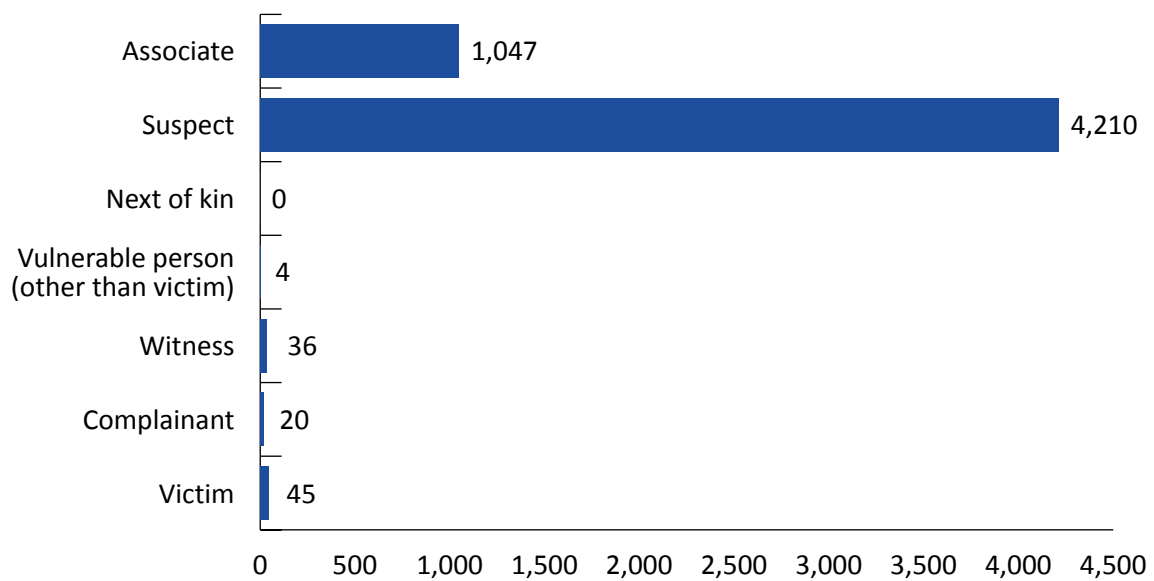
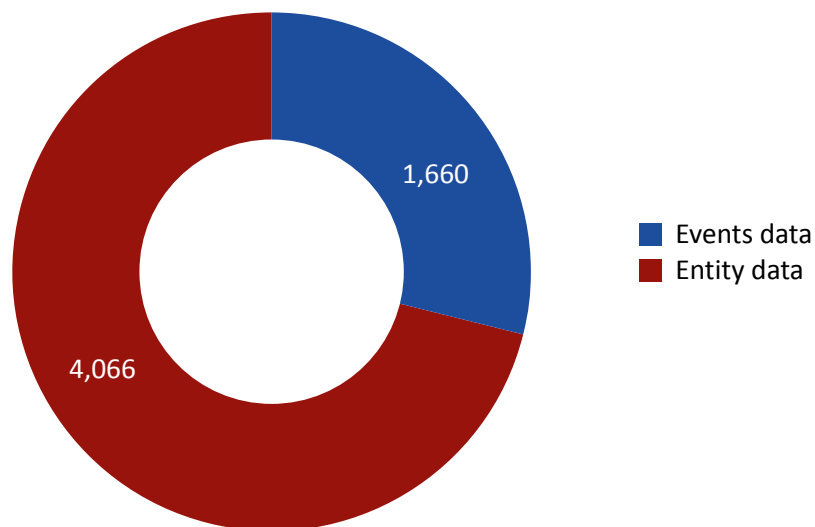
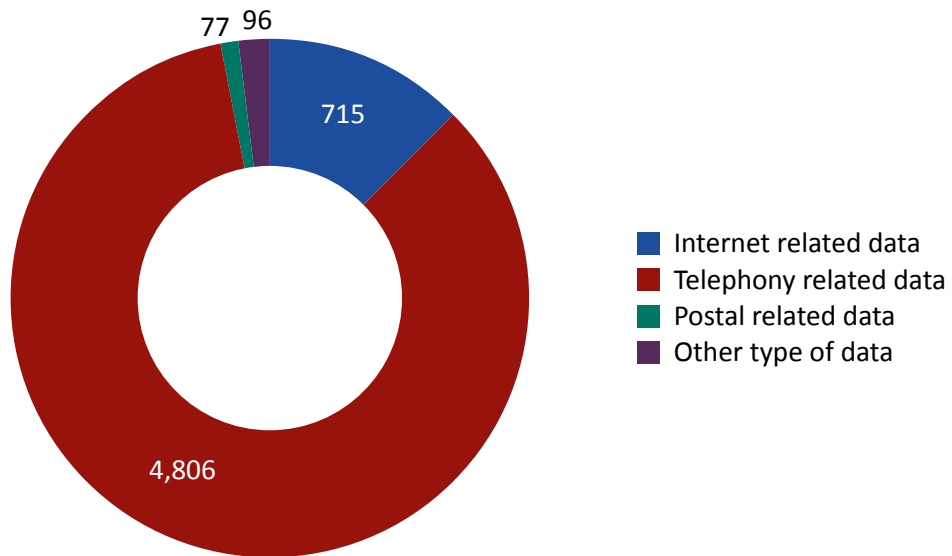
Figure 13: Communications data items by individual (subject), 2019**Figure 14: Communications data items by data type, 2019**

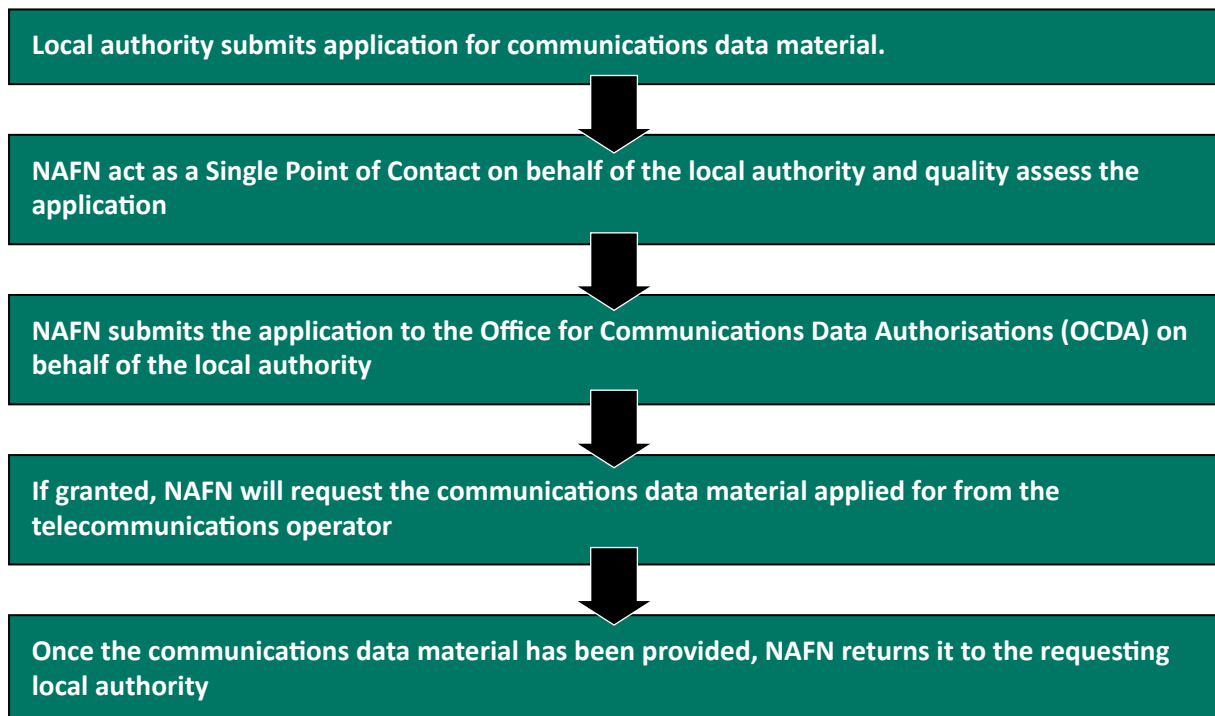
Figure 15: Communications data items by communications type, 2019



14. Local authorities

Overview

- 14.1 Local authorities may only authorise the use of directed surveillance, covert human intelligence sources (CHIS) or the acquisition of communications data (CD). Applications for CD are made via the National Anti-Fraud Network (NAFN). Both surveillance and CHIS authorisations require the approval of a magistrate in England, Wales and Northern Ireland.
- 14.2 We noted in our 2018 Report that we reduced the number of local authority inspections due to resource constraints. In 2019 we inspected 96 local authorities in relation to CHIS and surveillance powers and we plan to inspect all remaining local authorities by the end of 2020. Applications for the use of CD by local authorities are managed centrally at NAFN. From 2020, inspections will also address the adequacy of data retention safeguards at individual councils, noting that the IPA and the Codes of Practice (CoP) place an obligation on all authorities to ensure that any data they retain is stored properly. This will include any copies of CD material acquired via NAFN and, for example, saved on desktop computer systems. The process by which a local authority acquires material through NAFN is as follows:



Findings

- 14.3 Whereas operational activity is a core Law Enforcement Agency (LEA) function, local government personnel are far less frequent users of investigatory powers, particularly covert tactics such as surveillance or CHIS. In our view, such infrequent use raises the risk of staff becoming less skilled over time and we have found that it introduces a general fear of using powers incorrectly. The growth of local authority use of the internet and social media to engage with their communities brings the further risk that private information made available on social media platforms will be reviewed or monitored by council personnel without due consideration for privacy implications. The use of more conventional surveillance tactics, such as the use of covert cameras and test purchase, continues to decline and only a handful of local authorities used these powers in 2019.
- 14.4 Councils are increasingly favouring overt methods of investigation, for example using mobile CCTV to deter fly tipping at local hot spots. We have found that the long-term reduction in financial resources available to local government and increasing demands placed upon them means that greater emphasis has been placed on collaborative working arrangements, in particular with local police. In previous Annual Reports, we have commented upon the chilling effect that the requirement to obtain a magistrate's approval in England, Wales and Northern Ireland has had upon the use of covert powers.⁴⁴ However, where applications are made, there is evidence that magistrates are actively ensuring that such powers are being used appropriately by refusing applications where overt methods would have been successful.
- 14.5 CD acquisition has been an area of significant potential change for local authorities through the introduction of the ability to obtain events data. This is a relatively powerful new capability and we would expect the value of this tactic to benefit councils over the coming years. As described below, we have generally seen that these powers are being used proportionately and that the central administration of application and acquisition processes are working well.
- 14.6 We rarely encounter resistance to our inspection process, although it is not unusual for us to need to make repeated requests for information in order to arrange physical or remote inspections. Most councils welcome the opportunity to discuss covert investigatory powers matters, even when they are not using the powers available to them on a regular basis. We encourage all councils to provide introduction and refresher training to key personnel such as Authorising Officers (AOs) and investigators on a regular basis and to undertake awareness raising activity among wider council employees. As council staff become more familiar with the available powers, and better understand how they may be used during investigations, they become more confident to use them. Training is also the only effective mechanism by which staff can be taught how to operate within the law.

Covert human intelligence sources (CHIS)

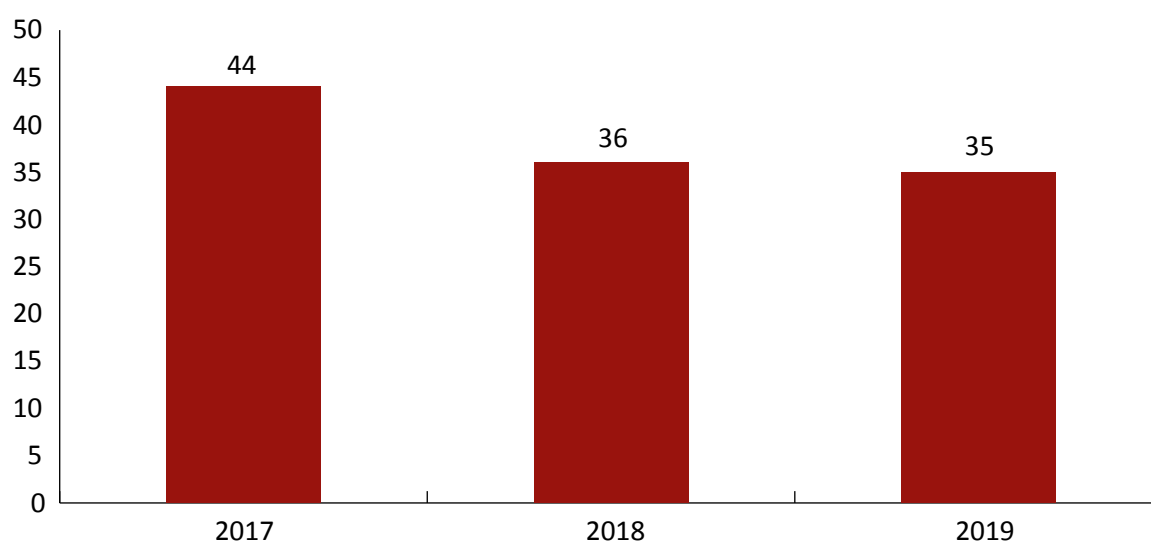
Regulation of Investigatory Powers Act 2000 (RIPA) policy

- 14.7 Our most common recommendations to councils refer to their RIPA policies. As noted in our 2018 report, we are still encountering RIPA policies that refer to the use of urgency provisions which were removed from use by local government in England, Wales and Northern Ireland by the Protection of Freedoms Act 2012. While this may seem a trivial

44 The Protection of Freedoms Act 2012 does not apply in Scotland and CHIS and directed surveillance activity is authorised under the Regulation of Investigatory Powers (Scotland) Act 2000.

matter, following these policies would likely result in a reportable error. In many of the authorities we inspected, the RIPA policy also fails to set out clear guidelines on the use of CHIS. It is common for councils to express a view that they would not consider using CHIS because they perceive the authorisation processes to be complex and risky. Establishing clear processes for the authorisation and use of CHIS in policy and supporting this through the provision of scenario-based training, helps to allay these fears and familiarise investigative staff with the full array of covert tactics available for their use.

Figure 16: CHIS authorisations for 2017 to 2019



- 14.8 Conversely, we commonly recommend that RIPA policies should contain guidance to ensure that daily interaction by council staff with members of the public does not inadvertently stray into CHIS territory. For example, where a member of the public makes a complaint about antisocial behaviour, they should not be asked to utilise a relationship covertly to obtain information about possible criminal offences because this amounts to the tasking of a CHIS.

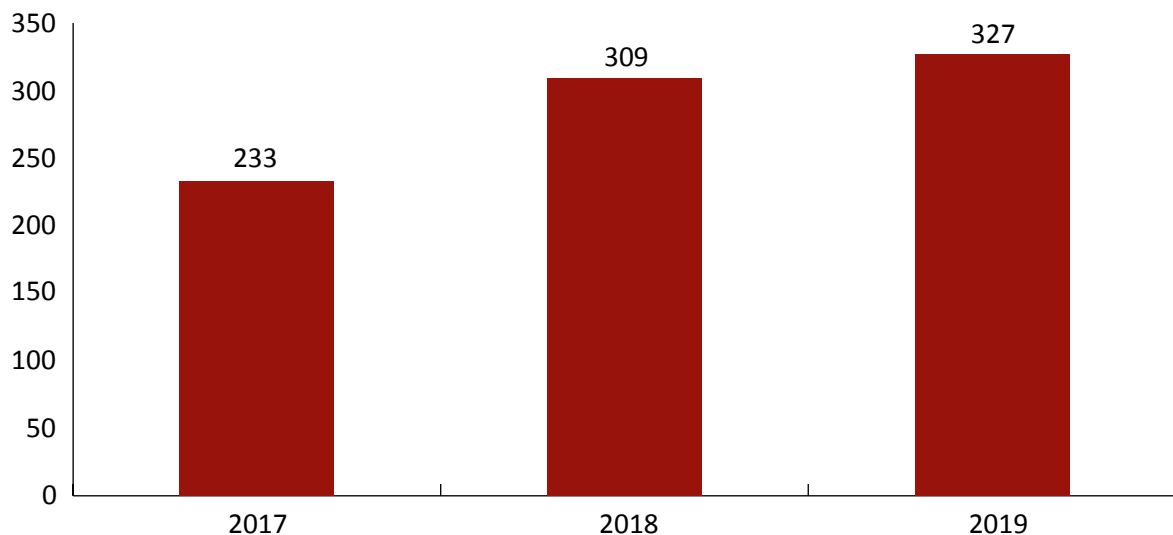
Internet and social media

- 14.9 The use of the internet and social media by local government has brought about the increased risk that private information available online may be accessed for investigative purposes. We encourage councils to use the internet as a legitimate information source in a responsible and structured manner. Each council's RIPA policy should clearly state the limitations in place on the use of information found on the internet for investigative purposes.
- 14.10 One council we visited during 2019 had undertaken a comprehensive audit of its internet use before introducing a firewall preventing council staff from accessing social media websites without first seeking permission and justifying their business need. While some councils may see this step as an overzealous restriction, it does help limit the potential for unregulated surveillance. It is not uncommon for council investigators to review online information on a one-off basis to confirm or refute suspicions or allegations. Such a brief review is unlikely to amount to surveillance, but we recommend that care should be taken to ensure that all research, be it one off or on an ongoing basis amounting to surveillance, is undertaken in a controlled manner and capable of being audited.

Surveillance

- 14.11 We have seen councils using covert cameras to identify and prosecute offenders for a range of crimes. For example, many councils have encountered an increase in the disposal of waste in unapproved locations by unlicensed businesses. This can sometimes amount to the systemic dumping of large amounts of material which is often harmful to the environment because it contains pollutants. Where overt methods such as mobile CCTV units have been unable to detect or deter suspects, the use of covert cameras has led to the identification and prosecution of offenders. We have seen that RIPA powers also provide an opportunity to investigate the sale of counterfeit, faulty or dangerous goods, for example by monitoring online sellers and using CHIS powers to engage with them to arrange the purchase, identification and seizure of goods.

Figure 17: Directed surveillance authorisations for 2017 to 2019



- 14.12 We have noted an increase in the use of directed surveillance to detect and prosecute cases of housing fraud. This most commonly takes place where a council has reason to believe that a tenant has breached the terms of their tenancy, for example by no longer living at, and sometimes sub-letting, their property. While this activity in itself is not sufficient to meet the crime test set out in the Protection of Freedoms Act 2012, where the tenant makes an application for right-to-buy they commit a fraud often leading to substantial financial loss. In such cases, surveillance has been used to show that the application has been made falsely and can produce evidence that is difficult to refute.

Example: use of RIPA tactics

One of the most striking examples we have seen of the innovative use of RIPA tactics was an investigation into two fraudulent companies undertaking dangerous heating, plumbing and drainage work. Following complaints by elderly and vulnerable victims, the local authority undertook a covert investigation during which they discovered that both businesses were owned by the same person who was knowingly defrauding them. This led to convictions for fraud and laundering the proceeds of crime.

Online surveillance

- 14.13 We frequently ask what mechanisms councils have put in place to prevent unauthorised surveillance, particularly online, and an insufficient response will result in recommendations to improve their rigour in this area. We recognise that there is a temptation for council staff to access private information online utilising council-provided or personal devices, and it will never be possible for us to know the full extent of such activity. We have been made aware of one case where a member of council staff conducted online enquiries for a protracted period and conducted their own private surveillance activity, all of which was unknown to their supervisor until it was identified and reported by a colleague. In this case, the error was reported to us and internal disciplinary action was initiated by the local authority.

Reports to elected members

- 14.14 The Covert Surveillance and Property Interference CoP requires that a report be made to Council Members on the use of RIPA powers on a quarterly basis. Where this is a nil return, reports will often be made less frequently as part of annual compliance reporting, usually to Audit and Standards Committees. It is important that such reporting mechanisms are maintained to ensure that Members are afforded the opportunity to scrutinise the use of covert investigation powers as part of the democratic process, and to annually approve the local authority's RIPA policy.

Communications data (CD)

- 14.15 During 2019 new provisions under the IPA brought a significant change to how local authorities acquire CD. Previously under RIPA, councils could only acquire limited data to identify the user of a telephone (now known as entity data). Under RIPA,⁴⁵ prior approval by a judge or magistrate was required to validate an internal authorisation before CD could be acquired.
- 14.16 Local authorities can now obtain both entity data and events data (for example, call billing or cellular location details) if the appropriate thresholds are met. From 11 June 2019, the prior approval process no longer applied; all local authority applications seeking to acquire CD are independently considered by the Office for Data Communication Authorisation (OCDA) (see chapter 5).
- 14.17 Unlike the LEAs, the IPA and the CD CoP place further requirements on councils seeking to acquire CD. Under the Act,⁴⁶ local authorities must use the services of NAFN, which acts as a centralised single point of contact (SPoC) service. NAFN will quality assure an application to address any omissions or failings before submitting the application to OCDA. If the authorisation is granted by OCDA, the NAFN SPoC will acquire the CD from the relevant telecommunications provider and forward the data to the applicant from the requesting authority. Currently, of the 400 or so local authorities, there are 355 registered with NAFN but of those, only 65 sought to acquire CD during 2019.
- 14.18 We have seen that the requirement to use NAFN brings a number of benefits. Firstly, the role of the SPoC requires specialist training and continuous professional development to become proficient and competent. Maintaining an individual in this role in-house would be challenging for local authorities in terms of cost, and the low volume of applications

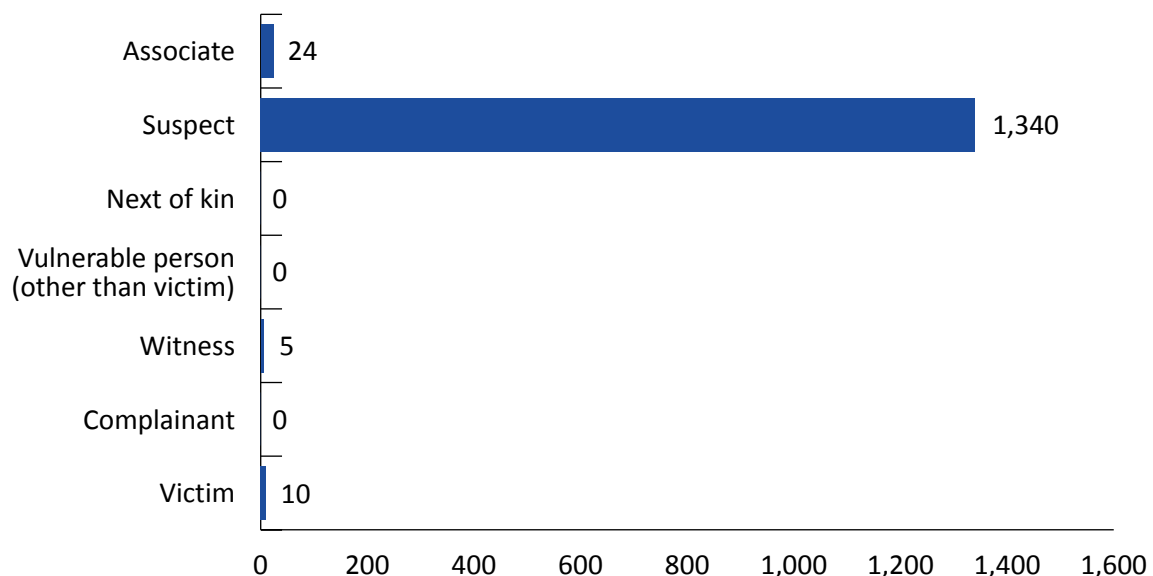
45 Sections 23A and 23B, as amended by The Protection of Freedoms Act 2012.

46 In accordance with section 73 of the IPA and as set out in paragraphs 8.1 – 8.7 of the Code of Practice.

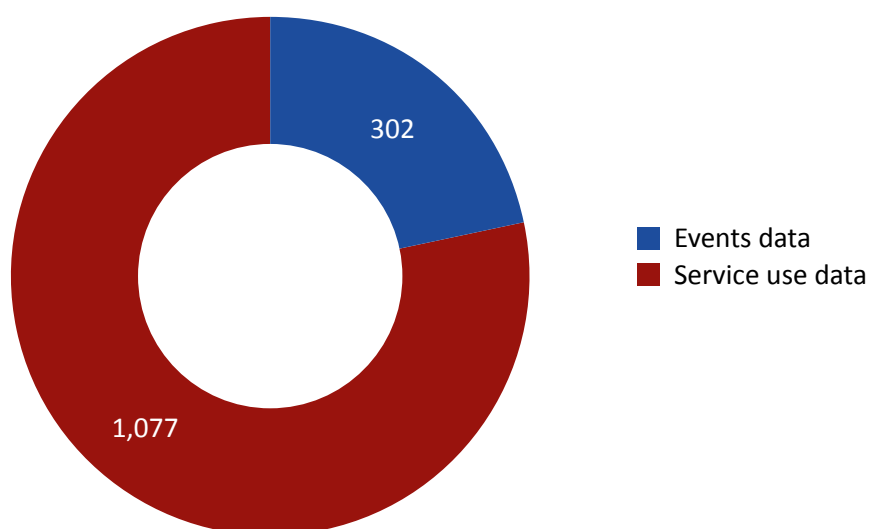
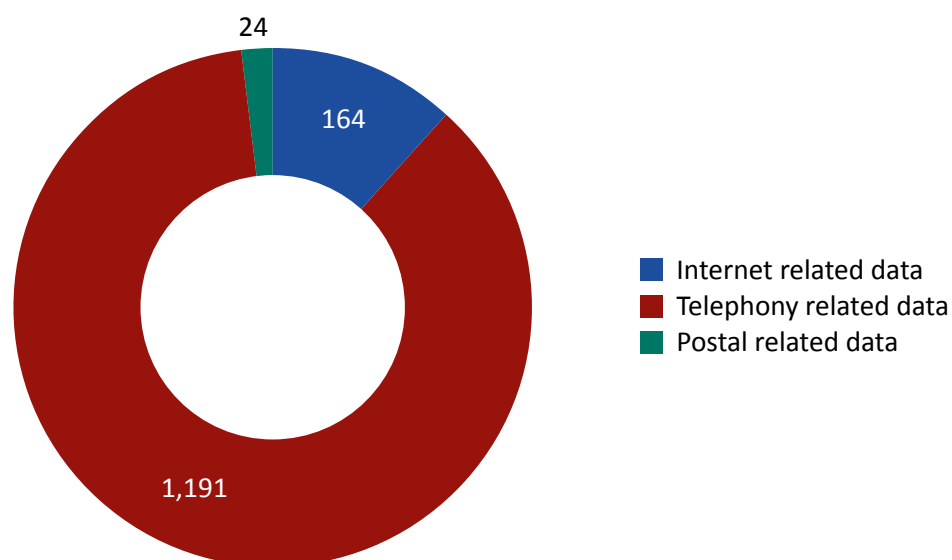
means gaining sufficient knowledge and experience would be difficult. Secondly, we can oversee all CD acquisition through a single, annual inspection of NAFN. This means that we can be assured that there is consistency of approach and that any recommendations or observations we make are applied nationally from the centre.

- 14.19 During 2019, NAFN processed 173 applications from only 65 local authorities indicating less than a half of those authorities who could seek to use CD did so. To address this and provide training and explanation of the changes brought about by the IPA, NAFN held a series of national roadshows at which presentations were given by our Judicial Commissioners (JCs) and Inspectors to emphasise the requirements of the Act and explain more about our inspection and oversight functions. As the circumstances in which CD can be sought by councils have widened, albeit only in accordance with an increased threshold of crime for events data,⁴⁷ we expect that applications for CD by local authorities will increase significantly during 2020 to supplement their use of RIPA powers.
- 14.20 Our annual inspection of NAFN identified a very good standard of process and quality assurance. During the inspection we examined application and acquisition records, supplemented by interviews with key NAFN staff such as the SPoC team, managers and legal advisors. We made no recommendations at NAFN for the second year running.

Figure 18: Communications data items by individual (subject), 2019



⁴⁷ Communications data that is wholly or partly events data may only be sought for the purpose of preventing serious crime. Entity data may be sought for the purpose of preventing or detecting crime or preventing disorder. A local authority may not obtain internet connection records for any purpose.

Figure 19: Communications data items by data type, 2019⁴⁸**Figure 20: Communications data items by communications type, 2019**

⁴⁸ Note that our 2018 report included similar figures, which were printed incorrectly. The 2018 figure should be 'Items of data by data type for local authorities in 2018'. The key is also wrong and assigns the colours to the wrong categories of data: subscriber information (647); service use data (87); and traffic data (0).

15. Prisons

Overview

- 15.1 Prisons are unique in our oversight because they are governed by different rules and legislation than apply to the other authorities we oversee. We inspect individual prisons as well as Her Majesty's Prison and Probation Service (HMPPS), the Northern Ireland Prisons Service (NIPS) and the Scottish Prison Service (SPS). We consider engagement with HMPPS to be critical to establishing and maintaining compliance across England and Wales; this has allowed us to address key issues centrally and to support the coordinated implementation of improvements across the prison estate in recent years.
- 15.2 In previous reports we have published statistics for prisons ratings, designating all prisons as 'good', 'satisfactory', or 'poor' for compliance. This reflected the way that our Inspectors were rating inspections for prisons only. On review, we found that the basis of these ratings was not robust and so have moved prisons onto a similar model to our other inspections. This means that no overall rating is used, but we consider the compliance of each prison and authority in relation to each relevant provision in the Investigatory Powers Act 2016 (IPA), Codes of Practice (CoP) and the Prison Rules 1999 (or equivalent in the devolved administrations). This methodology still enables us to identify poor performing authorities and to conduct follow-up inspections to investigate a specific issue, as necessary. In 2019 we conducted 125 prisons inspections.

Scottish Prison Service

- 15.3 On 16 April 2019, the Investigatory Powers Commissioner (IPC), the Cabinet Secretary for Justice and the Chief Executive Officer of the Scottish Prison Service reached agreement that the Investigatory Powers Commissioner's Office (IPCO) would implement a prison inspection regime of the Scottish Prison Service. IPCO would assess compliance with the legislation and procedures governing the use of interception of communications under the provisions of the IPA, the Prisons (Scotland) Act 1989, The Prisons and Young Offenders Institutions (Scotland) Rules 2011 and the Scottish Prison Rules (Telephones) Direction 2011. Inspections of all 15 Scottish Prisons took place between October 2019 and February 2020. These inspections will now occur on a yearly basis. Overall, we found that there was a good and consistent level of compliance.

Findings

- 15.4 We identified a significant decrease in the use of directed surveillance and authorised covert human intelligence sources (CHIS) across the prison estate during 2019, as shown in Figure 21 below. The decline in the use of directed surveillance reflects an increase in England and Wales of the use of Prison Rule 50A which allows for the overt monitoring of prisoners using CCTV. The management of rule 50A applications and authorisations now forms part of the IPCO inspection process for individual prisons.

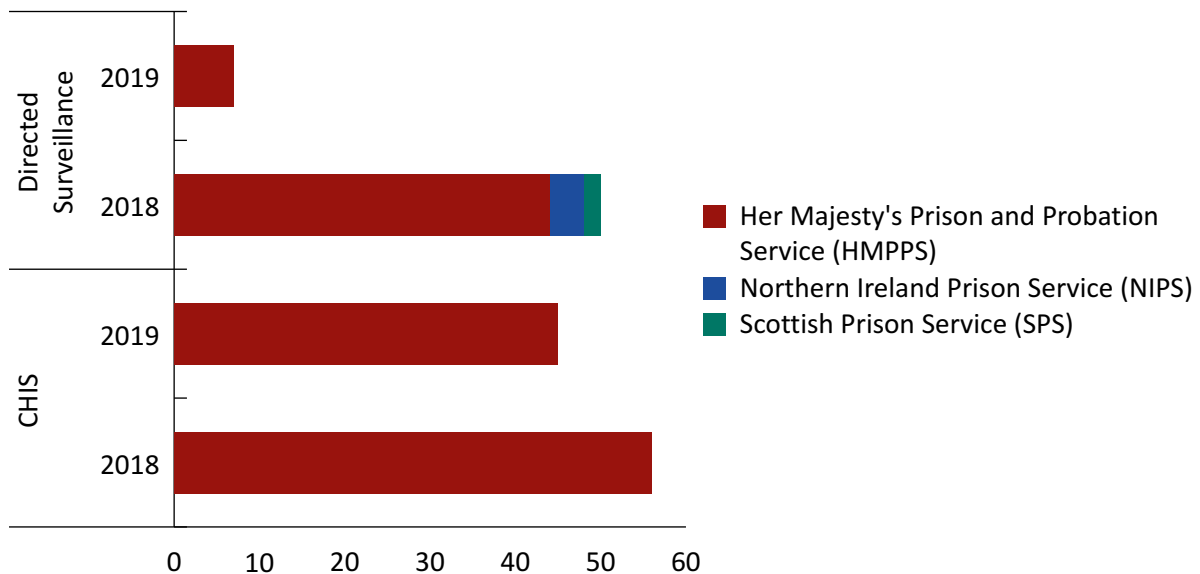
- 15.5 The ability for prisoners to communicate is undergoing transformation through the introduction of in cell telephones. This poses new challenges for prisons to ensure this does not pose a security risk and ensuring that the use of these telephones can be monitored in accordance with the Prisons Rules and the IPA. We found that HMPPS's management of this transition gave clear consideration to compliance and that overall the monitoring regimes within individual prisons are adequate.
- 15.6 Following our inspections of the Scottish prisons we made some recommendations and observations to tighten levels of compliance and improve practices and procedures for authorisation to monitor telephone calls and the retention of lists of telephone numbers. SPS informed us that all prisoners are given the opportunity to provide a list of telephone numbers for friends and family. Any calls to these numbers are preceded by an announcement that the call emanates from the Scottish Prison Service and alerts both the prisoner and person being called that the call will be logged, recorded and may be monitored. Prisoners are also asked to notify the prison of any phone number associated with legal representatives. This means that any calls to solicitors will be preceded by an announcement that the call will be logged but not recorded, allowing the prisons to be confident that they are not inadvertently monitoring and recording calls which should be subject to legal professional privilege (LPP) safeguards. This is good practice and alerts the prisoner and persons being called of the restrictions placed on the call, which safeguards their privacy.
- 15.7 In Northern Ireland, we found that Hydebank Wood College and Women's Prison and Her Majesty's Prison (HMP) Maghaberry and HMP Magilligan operate to a consistent standard and made a small number of recommendations and observations. At each, we recommended that they should adopt a consistent approach in using authorisations to monitor communications. This is not to suggest that the current approach is substandard; we found that all prisoners are fully informed about the arrangements for recording and monitoring their communications and how they can communicate confidentially with legal advisors and other bodies. We were pleased to note, additionally, that Hydebank Wood College has adapted this process to meet the needs of both the young offenders and female prisoners. Like in Scotland, the NIPS uses a recorded announcement to alert both the prisoner and the person called of the monitoring regime and we believe that this is good practice.

Covert human intelligence sources (CHIS) and surveillance

- 15.8 Running CHIS is always challenging and requires careful planning and monitoring to ensure that appropriate and reliable reporting is obtained while safeguarding CHIS welfare. Prisons present a uniquely challenging environment for such activity and we have raised concerns in recent years that considerations of necessity, proportionality and collateral intrusion in terms of CHIS management have been inadequately documented. In general, CHIS casework in prisons is not of the same standard as that kept by other authorities using powers of the Regulation of Investigatory Powers Act 2000 (RIPA) and this is an issue which we continue to discuss both centrally and with individual prisons. In 2019, we noted a general reduction in the number of active CHIS authorisations and a marginal improvement in the quality of the records we examined. We believe that focusing on fewer, but better run, CHIS will lead to an improvement in compliance which will likely also lead to operational benefits. We intend to monitor this trend during our 2020 inspections and will focus on the articulation of proportionality as well as the adequacy of handling and contact notes.

- 15.9 In 2018, we also highlighted concerns about the adequacy of training for Authorising Officers (AOs). We have not seen substantial progress in this area but understand that HMPPS intend that a regional restructuring, centralising the AO role, will improve this area by creating a smaller group of trained officials to review and authorise applications. This restructuring is described in further detail below.

Figure 21: 2019 CHIS and directed surveillance activity at HMPPS, SPS and NIPS.



- 15.10 The most recent inspection of HMPPS led to continued concerns regarding compliance levels. Policies and Prison Service Instructions remain outdated and newly proposed replacements still need approval and implementation. We found some improvement in the procedures adopted for the management of applications and authorisations. However, ongoing inconsistencies and consequential compliance issues demonstrate that there is still significant work to be done. The delay in implementing commercial software which has been purchased by HMPPS remains a frustration. The expected improvement in the operational competence of AOs has not materialised. HMPPS are aware of these concerns and their obligation to implement remedial measures.
- 15.11 HMPPS have proposed structural changes which would introduce a regional model. The concept of regionalisation of the application process for RIPA powers has been discussed over the last two years. This would create professional RIPA applicants and a small cadre of trained regional AOs, which would almost certainly have a positive impact on the compliance levels that currently exist. It is encouraging that the model has secured strategic support, funding from HM Treasury and that posts are being filled.
- 15.12 Despite the challenges HMPPS face, we have noted some impressive and inventive work during our inspections. A separate inspection of the HMPPS Digital Investigation Unit highlighted some innovative work and HMPPS are well placed nationally with regard to the use of the internet for investigative purposes. We hope that the policies and procedures that they have in place will enable this work positively to develop in the coming years.

CHIS in Scottish Prisons

- 15.13 We have found that the SPS has an excellent working relationship with Police Scotland regarding the management of CHIS in prisons. Members of the SPS are co-located with

Police Scotland colleagues and our examination of casework has identified that, as a result, applications are properly considered, covering current risks and taking into account already authorised CHIS. A nominated SPS authorising officer works closely with the relevant Police Scotland AO and authorisations will only continue with full concurrence from both. We found that this system works well.

Interception

- 15.14 The introduction of section 49 of the IPA did not result in any substantial changes to the interception of communications in prisons. Powers for prisons to carry out interception continues to be provided for under prison rules⁴⁹ on the grounds specified below:
- the interests of national security;
 - the prevention, detection, investigation or prosecution of crime;
 - the interests of public safety;
 - securing or maintaining prison security or good order and discipline in prison;
 - the protection of health or morals; and
 - the protection of the rights and freedoms of any person.⁵⁰
- 15.15 We oversee the appropriate security measures, safeguards and arrangements in place during inspections. Two of our key objectives are to ensure all interception and subsequent monitoring are carried out lawfully, and that the prisons are fully discharging their responsibilities to inform prisoners that their communications may be subject to interception. Prisoners' communications with their lawyers, Members of Parliament (MPs) and several other categories of individuals and organisations (such as the Samaritans) are 'privileged' or considered confidential and should not be read or listened to other than in the most exceptional circumstances. All other communications may be monitored.
- 15.16 Overall, the arrangements for the interception of communications are in accordance with prison rules and the Prison Service Instruction (PSI) 04/2016. There is a consistent approach to ensuring prisoners are informed that their communications may be subject to interception, and suitable measures are in place to configure the Personal Identification Number (PIN) phone systems⁵¹ to ensure that legal and confidential calls from prisoners are not recorded or listened to.
- 15.17 However, we identified several cases in which the documents, known as communications compacts, used to inform prisoners that their communications may be subject to interception were not legible and copies were rarely provided for prisoners to retain. While compacts were always signed by prisoners, some were not signed by staff to confirm that they had explained the contents as required by PSI 04/2016. We also found that the communications compact document was only available in one format with no alternative versions published by HMPPS to cater for individual needs, such as young offenders, foreign languages, visually impaired or dyslexic inmates. We have recommended that

49 Prison rules means any rules made under section 47 of the Prison Act 1952, section 39 of the Prisons (Scotland) Act 1989, or section 13 of the Prison Act (Northern Ireland) 1953.

50 Prison Rule 35A(5) of The Prison Rules 1999 confirms that "the protection of the rights and freedoms of any person" cannot be used to justify interception using a telecommunications system.

51 A PIN phone system allows a prisoner to use a Personal Identification Number (PIN) to make restricted calls to an approved telephone list only. All calls are recorded and stored for 90 days, except for those entered on the system as legal or confidential.

communications compacts are revisited by HMPPS and more suitable versions are made available for prisoners with specific requirements.

- 15.18 The ability for prisoners to make phone calls, send emails or write letters is important to maintain family connections and to access channels of help and support. The introduction of PIN enabled in-cell phones in some prisons has allowed calls to be made in private and at a time which fits with their families' schedules. In-cell phones also provide easier access to support services to improve rehabilitation and reduce the demand for illicit mobile phones.
- 15.19 However, safeguards must be in place to prevent inappropriate use of telephones and letters, for example, to contact victims of harassment or witnesses. Therefore, where public protection concerns exist, governors may authorise telephone calls and/or correspondence to be monitored routinely. Where there are security concerns, monitoring may be approved in order to gather intelligence or prevent crime. In both circumstances, the monitoring is authorised by a senior manager and must regularly be reviewed to ensure it continues to be appropriate.
- 15.20 Overall, we found that the authorisation process for monitoring both phone calls and mail were lawful. However, we identified several examples where the authorising senior manager failed sufficiently to explain why the monitoring was deemed necessary and proportionate, or why the decision had been made to continue or discontinue monitoring. If supporting evidence or intelligence had been considered during the senior manager's assessment, this was not always readily accessible to our Inspectors or recorded within the authorisation.
- 15.21 Prisons that have adopted a fully electronic workflow for their approval and monitoring processes were found to be more compliant in these areas than those that still relied on paper procedures. We therefore recommended that all prisons move to a fully electronic system with centrally shared access to relevant documentation for all personnel involved in the interception process. A key area for review during future inspections will be the implementation of a consistent policy for the retention, storage and destruction of intercept-related material as there was no consistent approach across all prisons.
- 15.22 Another key area for improvement that our inspections identified was that managers are rarely conducting enough random checks of PIN phone monitoring to provide assurance that staff who monitored telephone conversations did not exceed their remit. With limited resources, it is crucial that senior managers take a more targeted, intelligence-led approach and review the need for continuous monitoring more regularly. In addition, increased quality management checks should be undertaken to ensure monitoring has not been excessive. We will review whether there has been adequate improvement in this area in 2020.
- 15.23 As noted above, the SPS has configured their PIN phone systems to play a brief recorded announcement to the recipient to inform them that their call will be subject to recording and potential listening. However, there was no consistent arrangement in place for prisons within England and Wales and the reliance is upon the prisoner to inform the recipient. A recorded announcement would remove the responsibility from the prisoner and provide an option for the recipient to consent to receiving the call. This would also provide an additional safeguard against inappropriate use, especially where public protection issues exist. We will examine this further with HMPPS over the coming months.

Communications Data (CD)

- 15.24 The acquisition and disclosure of communications data (CD) is managed through HMPPS Headquarters. This is primarily sought for internal criminal investigations, such as misconduct in public office, offences under the Offender Management Act 2007, theft and supply of illicit drugs. All requests for CD made by individual prisons are processed by the SPoC Unit within HMPPS, which has recently undergone a structural change to include open source investigations. This change has increased the Unit's capacity to conduct anti-corruption investigations, including by monitoring illicit use of social media. This has resulted in a 180% increase in requests for CD which shows the progress made by the unit in its efforts to combat corruption. Applications for CD are now being approved by the new independent authorising body, the Office for Communications Data Authorisations (OCDA).

Wireless telegraphy

- 15.25 In 2018, we reported that HMPPS was progressing work to update technologies used under the Prisons (Interference with Wireless Telegraphy) Act 2012. This work is still in progress. We are working with HMPPS as they deliver this ambitious programme to ensure that the resultant powers are used appropriately. We will therefore maintain good sight of how these technologies will be used once they are rolled out. We expect that this will improve the prisons' capacity to prevent the use of illicit mobile phones and will lead to an increase in wireless telegraphy applications, but do not expect to see any decrease in other available powers in the medium term.

16. Warrant Granting Departments

Overview

- 16.1 The completion of the transition to the Investigatory Powers Act 2016 (IPA) has changed our relationship with the warrant granting departments, because the Investigatory Powers Commissioner's Office (IPCO) is now involved in the approval chain for most authorisations reviewed by the Secretary of State, as well as being responsible for retrospective oversight. Notably, this change has given our Judicial Commissioners (JCs) an insight into the pre-authorisation challenge function provided by the Secretary of State and through the warrant granting department (WGD). In many cases, and in the majority of novel and contentious cases, there is some additional dialogue between the WGD and the requesting agency to ensure that the requirement outlined is necessary and proportionate. We have seen that this scrutiny provides granular challenge which allows the WGD to review whether the proposed action will meet the required operational or intelligence outcome. This is of particular note for thematic authorisations where, before submitting an application to the Secretary of State, the WGD will ensure that the scope of the warrant is the minimum necessary to meet the stated aims. Much of our work at WGDs in the last year has been in this area.
- 16.2 The introduction of the new processes brought additional documentation. In our oversight capacity, we have observed that all WGDs should implement a policy to deal with the retention and disposal of IPA documentation.
- 16.3 We conducted one inspection at each department, reviewing casework across the powers they authorise. At the Home Office and Foreign and Commonwealth Office (FCO), this meant that we covered interception, equipment interference and bulk powers under the IPA as well as property interference and overseas powers under the Intelligence Services Act (ISA). At the Northern Ireland Office (NIO), we inspected interception and equipment interference and, at the Scottish Government, interception. The differences are due to the intelligence agencies or law enforcement bodies that use the respective WGDs and the powers available to them, as well as the fact that the Scottish Government is not involved in national security authorisations.

Findings

Home Office

- 16.4 Because of their role overseeing domestic authorisations originating from the National Crime Agency (NCA), Her Majesty's Revenue and Customs (HMRC), the Metropolitan Police Service (MPS) and MI5, the Home Office is the largest WGD and deals with the greatest volume of applications. This number has only increased under the IPA and our oversight has examined how well the unit has responded to this increased demand. In 2019 our inspection focused on the advice given to the Home Secretary in addition to the application submission. We saw regular challenge from the National Security Unit (NSU), often seeking

clarification and additional detail from the requesting agencies before the application was submitted to the Home Secretary. We consider this to be an invaluable part of the approval process, and the NSU demonstrated a commitment to ensuring that the information submitted to the Secretary of State is clear and accurate.

- 16.5 Our 2018 inspection of the Home Office's National Security Unit (NSU) focused on the scrutiny they provide throughout the lifespan of interception operations. The Home Secretary may impose conditions for review when approving any authorisation, for example where it is judged that there may be an unusually high level of intrusion into the target's privacy. However, we noted a number of cases where the requirement for review was not enforced and MI5 did not provide a relevant update at the designated time. We are pleased to see that both the Home Office and MI5 have improved in this area in 2019; the inspection found that all requested reviews were completed satisfactorily and in a timely manner.

Foreign and Commonwealth Office (FCO)

- 16.6 The FCO is responsible for approving warrant applications from the Government Communications Headquarters (GCHQ) and the Secret Intelligence Service (SIS), many of which will relate to activities conducted overseas which are not subject to the double lock. The introduction of the IPA required significant resources from the FCO to manage the new authorisation regime, which included a number of domestic applications and applications relating to bulk powers. This transition included an overhaul of the department's central records for warrants and authorisations which, as expected, assisted our oversight. Our 2019 inspection of authorisations at the FCO noted good evidence that the Foreign Secretary and senior officials provided appropriate challenge to the requesting agency in some difficult and complex cases. During this inspection, we scrutinised documented correspondence between the FCO and requesting agency, which recorded examples of the FCO challenging the scope and intrusiveness of proposed authorisations. We have no concerns about the standard of scrutiny or challenge provided in those areas.

Scottish Government and Northern Ireland Office (NIO)

- 16.7 The Northern Ireland Office (NIO) and Scottish Government routinely consider interception warrant applications from the Police Service of Northern Ireland (PSNI) and Police Scotland (PS) respectively. Both the NIO and the Scottish Government can receive interception warrant applications from the NCA, HMRC and MI5. Additionally the NIO considers ISA and other IPA warrant applications made by MI5 in relation to their Northern Ireland-based operations. The WGDs of the Scottish Government and NIO are providing a robust guardian and gatekeeper function for IPA applications in their respective areas. We saw a good level of compliance with the Act and the Codes of Practice (CoP). There was clear evidence of challenge and of early reviews being requested where appropriate and importantly that these reviews were done and scrutinised.
- 16.8 In 2018 we criticised the collateral intrusion statements made by Police Scotland and recommended that there should be greater consistency in some applications. We suggested that this was an area the Scottish Government should focus on in the future. In 2019 we facilitated a workshop in Glasgow with the Scottish Government and Police Scotland where this area was addressed and in the subsequent inspection we saw a marked improvement in how collateral intrusion is addressed.

- 16.9 At the NIO we saw excellent use of the early review process which is in the CoP. There was clear evidence of early reviews being suggested by the WGD and requested by the Secretary of State, as well as good management and scrutiny of those reviews to ensure they were complied with, and that the reviews were relevant and acted upon.

17. Technology Advisory Panel

Overview

17.1 Section 246 of the IPA requires the Technology Advisory Panel (TAP) to make a report to the Investigatory Powers Commissioner (IPC) about the carrying out of the functions of the Panel. The IPC has agreed that he will make this report publicly available through his Annual Report. The full text of the 2019 report is as follows:

Foreword

The year 2019 was the first year in which the Technology Advisory Panel (TAP) was fully constituted and active. Both as part of its general induction, and to ensure it gives timely advice, the Panel has received a range of briefings, for example from the Security Services, the National Crime Agency, and Home Office agencies. These were extremely useful for the Panel's work, and we are very grateful for the constructive spirit in which they were carried out.

The TAP's primary responsibility is to advise the Investigatory Powers Commissioner and their office (IPCO). Most of the advice provided has been at IPCO's request, but where the TAP has chosen to give advice of its own volition, that has been equally accepted and welcomed.

The TAP also initiated a wider consultation on Metrics of Privacy, ways of measuring intrusions on privacy. It is working actively on extending its range of more outwardly facing activities designed to encourage and access research relevant to IPCO's work.

It has been very encouraging that other jurisdictions, particularly in the Five Eyes, have shown an interest in emulating the way that the TAP has been set up, and in the function that it fulfils. Overall, I hope and believe that the TAP provides a very important function in ensuring that the Investigatory Powers Commissioner has access to the best possible scientific and technological advice, and has done so on very limited resource, around one person-year in total.

I would like to pay tribute to the founding Commissioner Sir Adrian Fulford both for his unstinting support for the TAP and for his strong defence of the TAP's independence, including from IPCO itself. It has been an equal pleasure working with his successor Sir Brian Leveson, and with all the Judicial Commissioners and IPCO staff.



Sir Bernard Silverman FRS, Chair of the Technology Advisory Panel

Remit of the Technology Advisory Panel

- 17.2 The Technology Advisory Panel (TAP) was set up under the Investigatory Powers Act 2016 ("the Act") (paragraphs 246-247). Establishing and maintaining the TAP is a responsibility of the Commissioner but the TAP may also give advice to relevant Ministers. The TAP has a dual function under the Act: to advise about the impact of changing technology, and to advise about the availability and development of techniques to use investigatory powers while minimising interference with privacy. In the definition of the panel's remit, "technology" is taken to be interpreted broadly, to include all relevant areas of science and mathematics. The remit of the Panel does not extend to consideration of matters of law, partisan politics or moral philosophy. The TAP is not a decision-making body and its advice cannot constrain any decision of the Commissioner or of any part of the Government.

Membership of the Panel

- 17.3 The Chair of the TAP is Sir Bernard Silverman FRS, formerly Chief Scientific Adviser to the Home Office and Emeritus Professor of Statistics at Oxford University. TAP members during 2019 were: Professor Muffy Calder, Vice Principal and Head of the College of Science and Engineering at Glasgow University, and previously the Chief Scientific Adviser for Scotland; Professor Derek McAuley, Professor of Digital Economy in the School of Computer Science at the University of Nottingham, John Davies, who has an extensive technical background in both government and private industry roles, and Daryl Burns, who has worked in cryptography and cyber security for over 30 years and was Deputy Chief Scientific Advisor for National Security.
- 17.4 TAP members are remunerated at an agreed daily rate. During 2019 members contributed an average of 25 days each to TAP duties. The TAP is supported by a Secretary who is a part-time (50%) civil servant.

Activities undertaken by the TAP and its members during 2019

Meetings

- 17.5 Panel meetings took place in February, May, July, September and December.
- 17.6 Formal meetings between the Chair of the TAP and the Investigatory Powers Commissioner took place in May and November.

Publications

- 17.7 A Working Protocol for the TAP, agreed between the Commissioner and the Chair of the TAP, sets out the structure and functions of the TAP, as well as the basis of the working relationship between the TAP and the Commissioner's Office.⁵²
- 17.8 The report of the November 2018 Metrics of Privacy workshop was published.⁵³

52 TAP, "Working Protocol" (March 2019), [https://www.ipco.org.uk/docs/TAP%20working%20protocol%20\(25%20March%202019\)%20FINAL.pdf](https://www.ipco.org.uk/docs/TAP%20working%20protocol%20(25%20March%202019)%20FINAL.pdf)

53 TAP, "Metrics of Privacy Conference" (November 2018), https://www.ipco.org.uk/docs/Formal%20report_Metrics%20of%20Privacy%20Conference.pdf

Written and verbal advice

- 17.9 The TAP provided briefings and advice on the following topics among others:
- a) End-to-end encryption;
 - b) Unmanned aerial vehicles/drones;
 - c) Data integrity checks and Blockchain;
 - d) Hashing and Machine Learning;
 - e) Internet Connection Records.
- 17.10 Technical support was provided to inspections (including on issues that cannot be described at this level of classification) and a number of *ad hoc* queries by Inspectors and Judicial Commissioners were addressed informally. TAP members attended a variety of inspections in person.
- 17.11 The TAP provided crucial support to the Commissioner and IPCO during a serious compliance failure investigation, which had significant national security implications. IPCO investigated serious compliance risks associated with certain MI5 technical environments (see chapter 8); the TAP was requested to provide technical assistance to IPCO over an extended period. A member of the TAP was closely involved with the inspections which took place at MI5 and assisted the inspectorate in interviewing engineers and other technical experts at MI5 about the ways in which the technical environment was processing warranted data.
- 17.12 The TAP has contributed to IPCO's participation in GCHQ's Equities Process
- 17.13 TAP members were given briefings on Internet Connection Records (ICR) including the legislative background and operational context and the implementation plans for a trial of legal acquisition and use of ICRs for law enforcement purposes. They also visited the National Crime Agency (NCA) for further discussion and a demonstration of the communications data application process. The panel is keen to have continued involvement in the plans for technical development. The TAP provided guidance for IPCO staff on ICR.
- 17.14 The TAP held a meeting with the Head of the Accelerated Capability Environment (ACE), a capability mobilised by the Home Office. ACE/VIVACE works with over 150 entities from both academia and industry to tackle complex problems for security questions through innovation, engagement, collaboration and trust. This briefing covered the processes used to make innovative use of technologies and the forward-looking horizon-scanning work they undertake.
- 17.15 The TAP discussed various issues with the Chief Scientific Adviser for National Security, highlighting key research activities, industry and academic engagement as well as a presentation on the science strategy in the changing threat environment.
- 17.16 The TAP has participated in international activity, for example:
- a) the Five Eyes Intelligence Oversight and Review Council conference,
 - b) briefings for the Australian Inspector General and the Australian Independent National Security Legislation Monitor,
 - c) a conference in Copenhagen between several EU countries, sharing ideas and methodology and addressing issues relating to oversight and technology in different countries,

- d) a conference of the European Intelligence Oversight Network (EION) in Berlin. The TAP chair is interested to pursue whether the TAP could do some joint work with EION in future, potentially a collaborative workstream on the topic of automated anomaly detection.

18. Errors and breaches

Overview

- 18.1 Investigation of errors and breaches reported to us by the authorities we oversee is an important part of our work. We may also discover potential errors during the course of our inspections. These are then investigated by the authority concerned and formally reported to us. We investigate all matters reported to consider the impact the error has had on the human rights of any individual affected, and to consider whether the report reveals any failings in the processes and safeguards in place at that authority. Our website includes details about the type of errors we investigate and provides examples of the kind of issues we see.

Notable errors reported in 2019

MI5 compliance error

- 18.2 Full details of the compliance error identified by MI5 and our investigation into their failure to demonstrate adequate compliance processes across certain technology environments is given in chapter 8. We are confident that MI5's internal review of safeguards, initiated following the realisation of the severity of the issue, and the potential for this to have resulted in multiple errors in data handling, will identify any substantial vulnerabilities in their data handling model and lead to the elimination of errors of this kind in the future.

Her Majesty's Revenue and Customs (HMRC) covert human intelligence sources (CHIS) error

- 18.3 HMRC reported an error in relation to its management of witnesses who assisted in investigations and gave evidence in support of a small number of prosecutions. Over the course of several years, those investigating officers who engaged with potential witnesses failed to consider that many of these individuals were acting as CHIS and required authorisation. The cause of the error originated from a misguided policy which had, in turn, been misapplied by many officers involved in these operations. The public authority undertook a comprehensive review of current and historic investigations to identify the number of affected prosecutions. As the policy had been in force for approximately 15 years, a significant number of investigations were involved. Importantly, the number of cases where convictions had been obtained and such a witness was used during the investigation who should have been the subject of a CHIS authorisation was comparatively small; in single figures. It should be noted that the CPS has taken the view that none of the convictions secured was unsafe and that HMRC has fully discharged its disclosure obligations.
- 18.4 We have worked closely with HMRC, including conducting an interim inspection to focus solely on the remedial measures which have been implemented to avoid recurrence. HMRC

has withdrawn the original policy and replaced it with revised, legally compliant guidance which is available to all staff on their intranet. A significant investment in training related to the Regulation of Investigatory Powers Act 2000 (RIPA) has also been undertaken to raise awareness amongst staff of the provisions governing the lawful and effective use of human sources of intelligence. We expect these measures will ensure such errors are not repeated.

UK Intelligence Community (UKIC) errors

- 18.5 For 2019, the errors reported did not suggest systemic failures of safeguards or an attempt to act unlawfully or circumvent safeguards. The tables and graphs below are intended to enable comparisons to be made with performance over previous years. We consider the absence of any pattern of errors to be important, as this suggests that UKIC are not repeating known errors. In 2019 an unusual number of 'systems' errors were identified. We have used this category to describe errors with IT systems handling different types of data. The identification of some of these has stemmed from the intensive IT improvement work which followed MI5's compliance errors. Some other categories, such as bulk personal data (BPD) errors, have also increased for this reason, following work across UKIC to interrogate and improve their IT structures. Whilst it is very disappointing to note that several systems were not handling data as expected and in accordance with the requirements of the Investigatory Powers Act 2016 (IPA) and the Codes of Practice (CoP), we are satisfied that this work has initiated a significant improvement in how compliance is considered at all of the agencies.

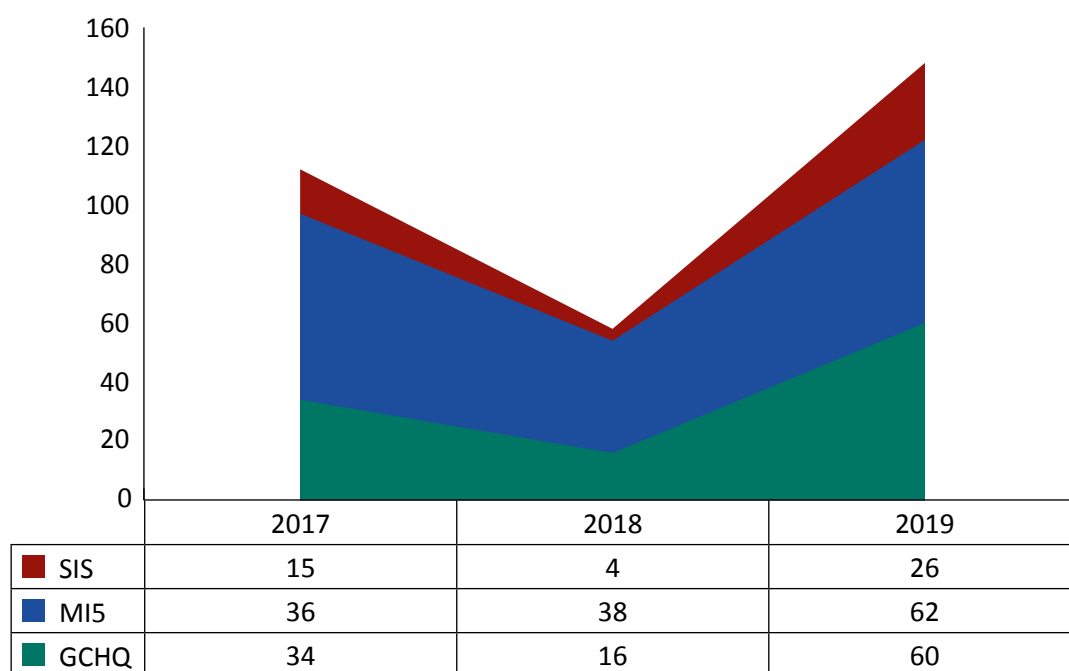
Table 2: UKIC errors, 2019

Powers	Agency			Total
	MI5	GCHQ	SIS	
Covert human intelligence source	5	0	9	14
Directed surveillance	13	3	0	16
Property interference	6	1	0	7
Bulk personal data	14	1	10	25
Section 7	–	1	0	1
Targeted interception	23	10	4	37
Bulk interception	–	41	–	41
Equipment interference	1	2	3	6
Bulk equipment interference	–	1	–	1
Communications data (reportable)	55	1	1	57
Systems	13	0	0	13
Total	130	61	27	218

- 18.6 A total of 218 errors were reported to us by UKIC in 2019. No errors were reported by the warrant granting departments (WGDs) or the Ministry of Defence (MOD). Comparison of these figures with previous years is complicated because the IPA has essentially re-categorised existing powers, and in some cases established a threshold for errors of those powers.⁵⁴

⁵⁴ Note that the figures printed for UKIC errors in 2018 were inconsistent within the report. 163 errors were reported in total. Of those, 122 were reported by MI5, 37 by the Government Communications Headquarters (GCHQ) and 4 by the Secret Intelligence Service (SIS).

Figure 22: UKIC errors by organisation, 2017 to 2019, excluding communications data and systems errors.



**Note that no errors were reported in 2019 by the MOD or WGD. Previous versions of the chart did not include CD and interception errors.*

Figure 23: Reportable UKIC communications data errors by organisation, 2018 to 2019

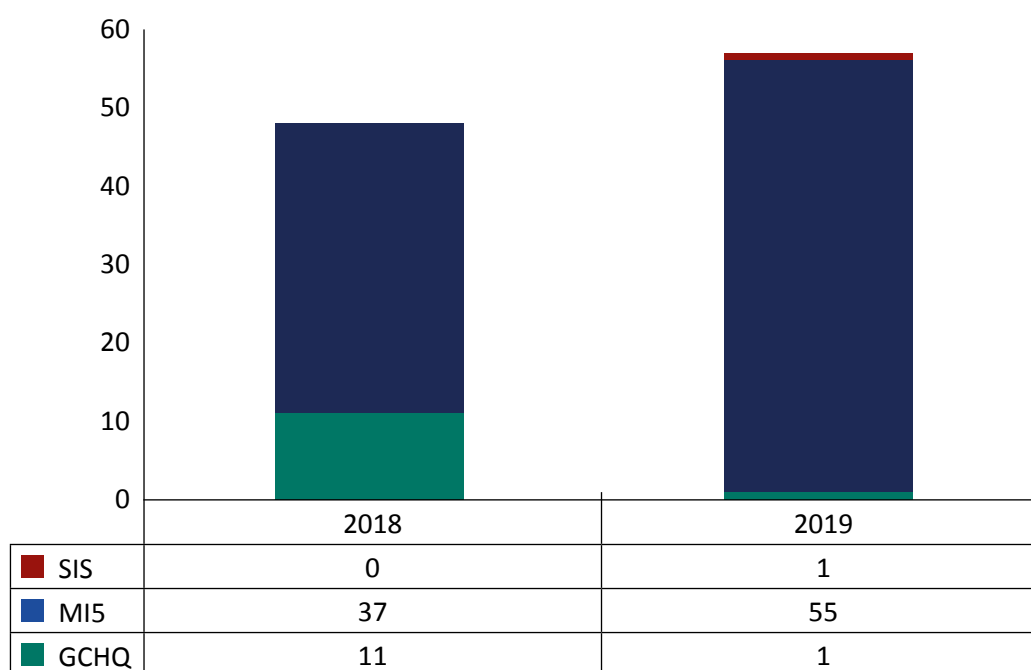


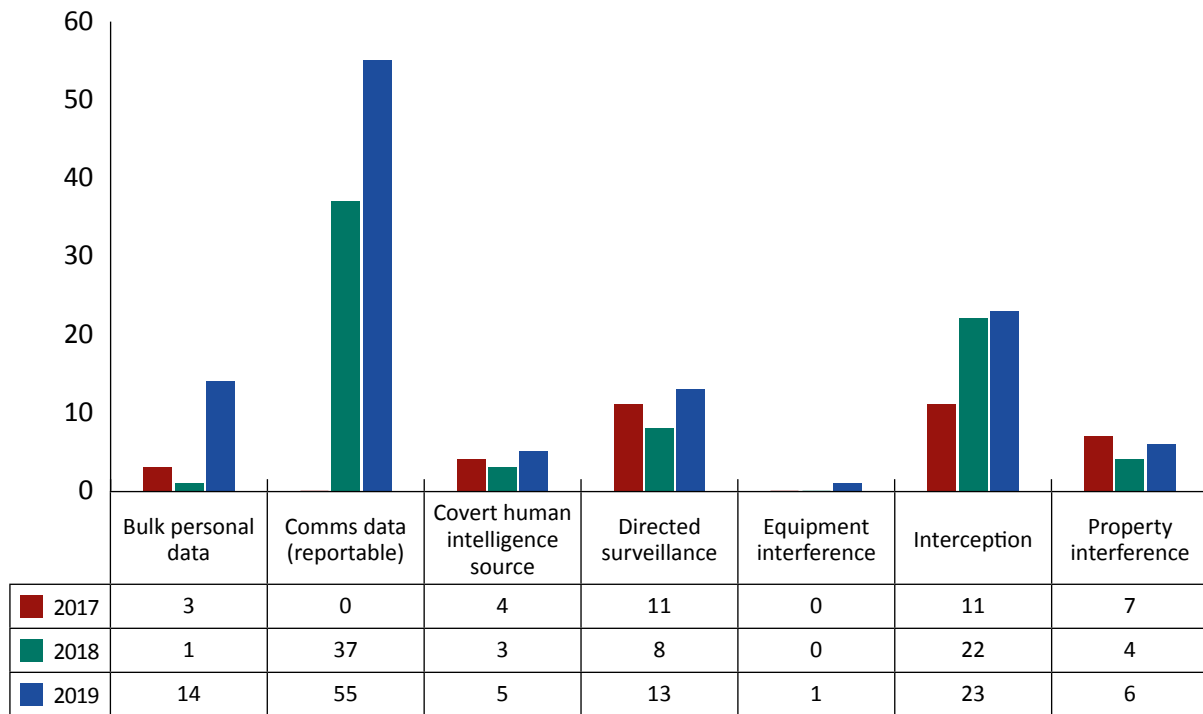
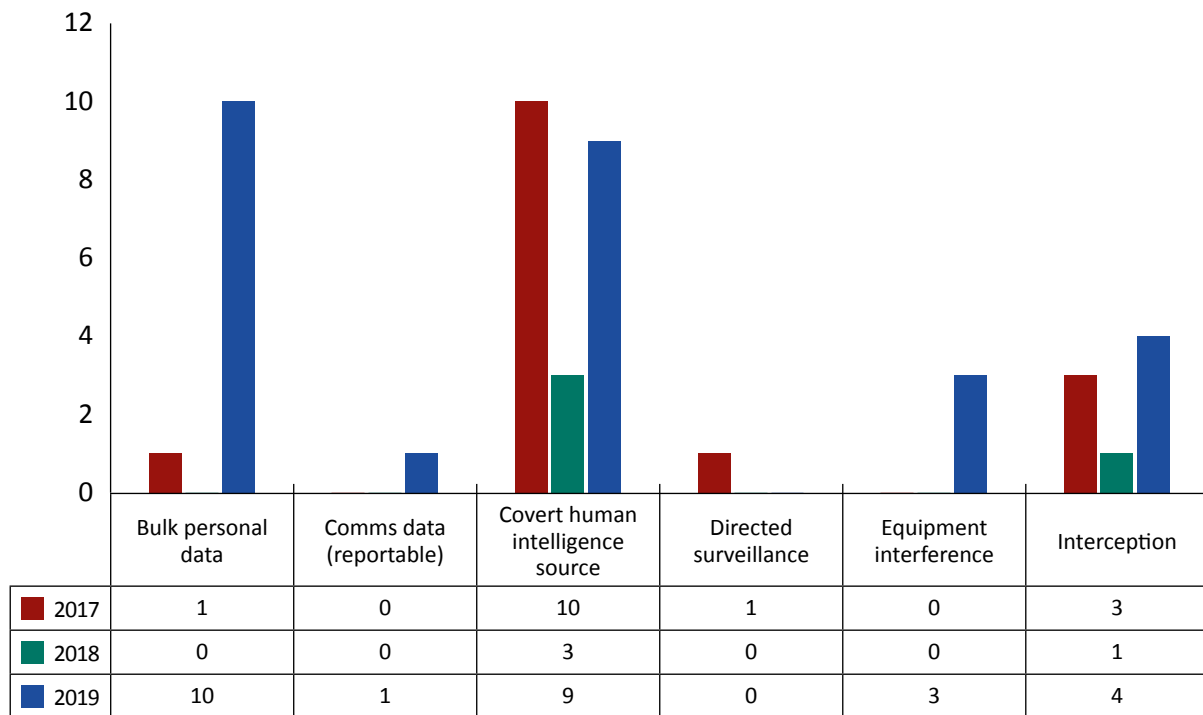
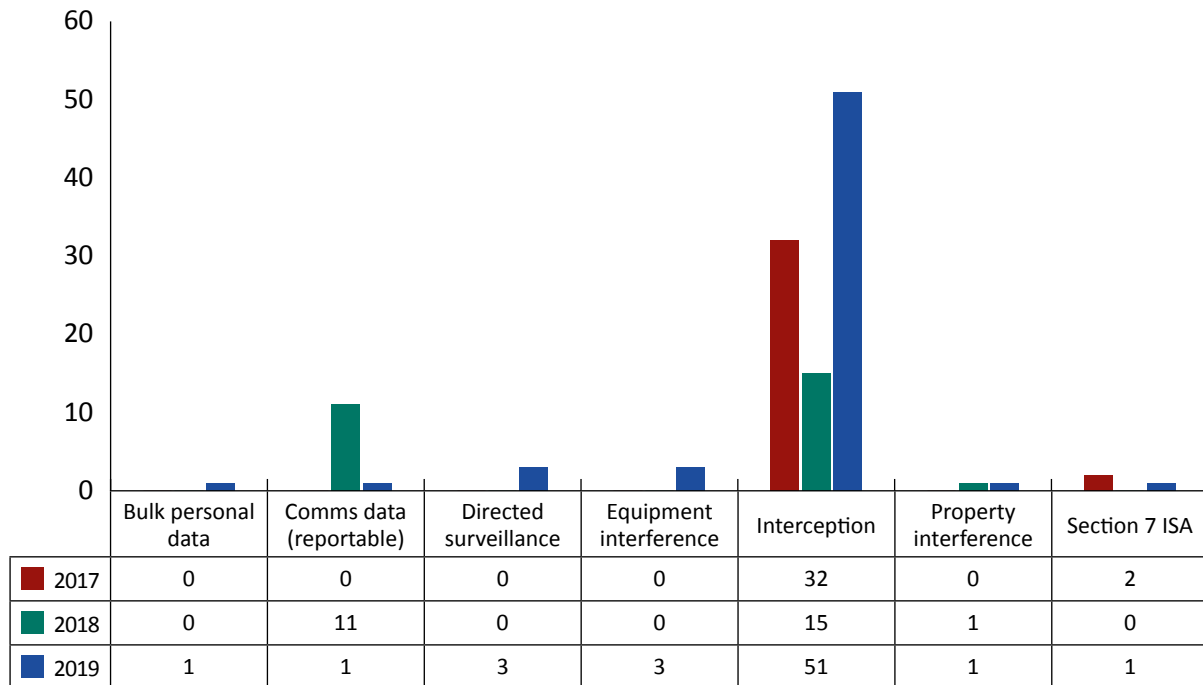
Figure 24: MI5 errors by type, 2017 to 2019**Figure 25: Secret Intelligence Service (SIS) errors by type, 2017 to 2019**

Figure 26: Government Communications Headquarters (GCHQ) errors by type, 2017 to 2019



18.7 In our assessment, although a higher number of errors were reported in some areas than in previous years, there is no general pattern of non-compliance following from errors reported in similar areas in 2017 and 2018. The greatest increases in reported errors were in BPD errors reported by both MI5 and the Secret Intelligence Service (SIS), and bulk interception errors reported by the Government Communications Headquarters (GCHQ) (see below). The number of BPD errors may reflect the fact that SIS and MI5 were implementing the new provisions and changes to the required processes and ways of working; we would not expect to see a similar figure for 2020. These errors were generally human errors, for example an officer searching for their own phone number rather than a target's by mistake. Other errors have been more substantial, such as where agencies have identified unwarranted BPD holdings; in each such case the agency either subsequently applied for a warrant or deleted the data. Errors of this kind have led us to give more attention to the data-holding systems at each agency and this will continue to be a focus in coming years.

18.8 The nine CHIS errors reported by SIS is higher than we, or SIS, would expect to see in this area. Most of the CHIS errors reported by SIS related to agent cases or operations conducted under the Intelligence Services Act (ISA) but where a period of activity met the criteria for authorisation under RIPA and where this change in circumstances had not been recognised. There was no suggestion of deliberate neglect, rather a lack of understanding of when a RIPA authorisation was required. The remaining errors occurred when an authorisation was allowed to lapse when it was still required. The increase in reported errors during the year reflects at least in part a greater ability by SIS to recognise when errors have taken place. SIS has designated a member of staff to help improve RIPA compliance and we expect to see a significant fall in such errors in 2020.

- 18.9 Last year we provided statistics for recordable UKIC errors in relation to CD acquisition (see below).⁵⁵ UKIC are not required to formally report these figures to us and we have not collected them this year.

Interception: UKIC and Law enforcement

- 18.10 This year has seen an increase in errors reported to the Investigatory Powers Commissioner's Office (IPCO) by GCHQ from 15 to 51. The 51 are broken down as 10 Targeted Intercept and 41 Bulk Intercept. Whilst the apparent increase is large, we should note that these are all now classed as reportable errors. Reportable errors is a term introduced and defined for the first time in the IPA and accompanying Codes of Practice and there was no such definition for lawful intercept in RIPA. This year is the first full year of IPA so there is no direct comparison to previous years, although it is clear there has been an increase and we will carefully monitor the trend. Another major contributing factor to the larger number of errors is the change in working practices within GCHQ. They have invested in resource, technology and systems to improve their ability to identify, trace and fix errors that are mainly caused by complex data flows. A rise in numbers was anticipated as they developed better methods for finding and fixing errors. It is not possible accurately to say if these errors were happening before but undetected, but now that we have a new baseline we will be able to track this in future through oversight and inspection.

Definition: recordable error

A recordable error is defined by the relevant Code of Practice and is one that has been identified by the agency without any data being incorrectly acquired or disclosed. A list of recordable errors is retained by an agency. The record explains how the error occurred and provides an indication of the steps taken to prevent a reoccurrence. At each inspection, the list of recordable errors is audited and, if necessary, observations or recommendations are made in inspection reports to tighten procedures or processes. An example of a recordable error is when an analyst manually transfers data to a system and inputs the information incorrectly, making a transposition error which does not result in the acquisition of incorrect data.

Definition: relevant error

Section 231(9) of the IPA defines a 'relevant error' as an error: a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner; and b) of a description identified for this purpose in a code of practice under Schedule 7.

Definition: serious error

Section 231(2) of the Investigatory Powers Act 2016 (IPA) defines a serious error as one where significant prejudice or harm has been caused to a person as a result of a relevant error.

⁵⁵ Note that the figures printed for CD errors for 2018 were incorrect. The total number of communications data errors, including recordable and reportable errors, for UKIC for 2018 was 104, of which 84 were related to MI5, 20 to GCHQ and none to SIS.

- 18.11 There was a significant increase in the number of interception errors reported by five law enforcement agencies (LEAs) in 2019 compared to 2018. LEAs reported 24 relevant⁵⁶ errors in 2019, compared to 13 in 2018. While the threshold for reporting errors is broadly similar, 2019 is the first full year of capturing relevant errors so again there is no direct comparison to previous years. While this increase is potentially concerning, our investigations to date have suggested that this increase may have resulted from the introduction of formal error definitions under the IPA. Each agency is required to record regular reviews in relation to interception errors.⁵⁷ We will examine these records at our 2020 inspections and probe whether appropriate measures have been introduced to prevent the repetition of similar errors throughout 2020.
- 18.12 There were no serious errors reported in 2019 in relation to interception.
- 18.13 Once a public authority establishes that they have committed a relevant error they must report it to the Investigatory Powers Commissioner (IPC) within ten working days. An Inspector will then investigate the circumstances that led to the error. In all the relevant errors that were reported in 2019 we are satisfied that the agencies concerned have taken reasonable steps to mitigate the risk of reoccurrence of the same type of error: most of the relevant errors reported in 2019 related to administrative process issues.
- 18.14 The most common error on interception related to the collection of material beyond the point of authorisation. In several cases, there was a delay between the authority notifying the telecommunications operator (TO) and the data flow from the intercepted device being stopped after the warrant had been cancelled. Typically, this latency resulted in up to 48 hours of unauthorised collection, although technical safeguards at each relevant authority meant that that data was not ingested into monitoring systems for analysis.

Data handling errors relating to interception material

- 18.15 In mid-2019 the National Crime Agency (NCA) notified us of two data handling errors which they had identified during an internal review. The NCA briefed us on an ambitious internal review programme which they had conducted following discussions about the adequacy of safeguards on corporate systems with MI5 (see chapter 8). The first error related to the unintentional retention of interception metadata in a pilot system which had been used to test a potential capability. While this data was retained, it was not accessed by NCA staff and has now been deleted.
- 18.16 The second error involved the retention of warrant related casework for interception for longer than the required five-year period. The NCA reviewed all warrant casework records and identified those that had been retained longer than the necessary period before deleting them. We were pleased to note that the NCA also conducted a comprehensive systems review and did not identify any similar errors in relation to data handling. Like MI5, the NCA has taken the opportunity to review and strengthen safeguards to better enable them to monitor and demonstrate compliance with RIPA and IPA safeguards.

Interception errors reported by non-intercepting authorities

- 18.17 During the year, we received four error reports in relation to police forces without interception powers. Two of these errors occurred when the TO had provided material that

⁵⁶ A relevant error is defined in section 231(9) of the IPA and in 10.12 to 10.16 of the Codes of Practice.

⁵⁷ Paragraph 10.10 of the Code of Practice states: "A person holding a senior position within each intercepting authority must undertake a regular review of errors and a written record must be made of each review."

constituted interception product in response to a communications data request. While this is concerning, we are encouraged by the proportionally negligible number of these errors, in the context of the volume of CD requests, and the fact that the relevant police forces immediately identified and notified us of the error, while deleting the erroneously obtained material. We expect that the structured approach to CD requests, established through the role of the Office for Communications Data Authorisations (OCDA), in ensuring that CD requests are accurate and standardised, means that similar errors are unlikely in the future. However, we are aware that a number of small TOs remain unfamiliar with the processes and safeguards in the IPA, which means that there is a risk of similar instances happening in future.

- 18.18 The two further errors were caused when police forces conducted authorised telephone downloads and inadvertently obtained live communications content, which constitutes interception. As described elsewhere, we are working with police and national bodies to support work by the police to use their equipment interference powers appropriately.

Surveillance, property interference and covert human intelligence sources (CHIS): Law enforcement agencies (LEAs), public and local authorities, and prisons

- 18.19 Errors continue proactively to be reported by the authorities we oversee, with only 6 errors in this category being discovered during LEA inspections in 2019. We judge that this indicates that error reporting is an open and transparent process embraced by authorities, and that the process set out in section 235(6) of the IPA is working well. The number of errors, in proportion to the number of authorisations and renewals granted in 2019, continues to be low. As in previous years, our investigations have not identified any authority to have systemic failings in their application of the legislation and guidance for the use of covert investigative techniques. We did not see the repetition of similar errors which would otherwise suggest that processes across various authorities are inadequate. None of these errors when examined were found to constitute a serious error as defined under section 231 of the IPA, in that no significant prejudice or serious harm was suffered by any individual as a result of those errors

Table 3: Total surveillance, property interference, covert human intelligence sources (CHIS) and equipment interference errors for law enforcement agencies (LEAs), public and local authorities and prisons for 2019

Investigatory Power	Number of Errors
Directed Surveillance	66
Property Interference	9
Intrusive Surveillance	4
CHIS (including undercover officers)	9
Equipment interference	8

Law enforcement

- 18.20 In 2019, 85 errors relating to surveillance, property interference, CHIS and equipment interference were reported by LEAs. The number of errors is consistent with that reported last year, with the vast proportion relating to the powers associated with directed surveillance and observation activities going beyond that which was authorised. As detailed

in chapter 12 we have reviewed the adequacy of processes and policies in place to prevent continued occurrence of errors of this kind.

- 18.21 The vast majority of errors stemmed from human mistakes, either from a misunderstanding or lack of awareness of the activity which had been authorised, or from covert activity which had continued beyond a cancellation or expiry of an authorisation. In all cases, after further investigation by the public authority, or by an Inspector, additional administrative measures or training have been introduced within the organisation to ensure that there is no repetition. Should errors continue to be repeated within an organisation we will prioritise investigating the issue at our next inspection.
- 18.22 Errors in online directed surveillance has been a focus of our attention in 2019. In 2018, we noted concerns that new and developing capabilities to monitor social media activity online might result in a high proportion of errors resulting from surveillance without proper authorisation. Fortunately, we have not found this to be the case and only five errors of this kind were reported in 2019. We found that this relatively new methodology has been appropriately deployed and robustly monitored within organisations. We examine the relevant policy and procedures at each surveillance inspection to ensure that appropriate audit structures are in place; this allows suitable oversight and provides assurance that the tactic is being used in a lawful and compliant manner. We have found that the pattern of errors is in line with those occurring in traditional directed surveillance operations, largely aligned to human error and a lack of awareness of the parameters within authorisations.

Public authorities

- 18.23 Seven directed surveillance errors were reported by public authorities. These all related to directed surveillance having been conducted without appropriate authorisation.

Local authorities

- 18.24 Errors caused by local authorities are rare, which is to be expected given the low number of authorisations sought and relied on by councils conducting investigations. Where they do arise, this is often either due to inadequate policy and processes or because of a lack of awareness of, or willingness to abide by, guidance on the use of CHIS or surveillance. During 2019 we were made aware of one error where a local authority had undertaken surveillance utilising static cameras placed outside the home address of persons reporting that they had been the victim of harassment and anti-social behaviour. A second error reported to us by a different local authority related to the use of CHIS without appropriate authority. In both cases no authorisation was sought; it appears that this was due to a lack of suitable policies and processes to facilitate authorisation.

Prisons

- 18.25 There were two errors reported by prisons in 2019, one by Her Majesty's Prison and Probation Service (HMPPS) and one by an individual prison. Although there is no obligation to report errors for surveillance conducted under Prison Rules, we encourage error reporting as best practice. No errors were reported regarding other investigative powers and, as with all low-reporting authorities, it is important for us to consider whether such figures reflect a failure to recognise and or report errors, which would be of significant concern. However, we judge that the low number of RIPA, surveillance and CD authorisations relied on by prisons means that this is proportionate to the error rates we are seeing reported elsewhere.

Communications data (CD) errors: law enforcement agencies (LEAs), public authorities and prisons

- 18.26 The IPA (section 231(9)) specifies that only a public authority may cause a relevant error. This would exclude an error resulting from mistakes made by a TO, despite the possibility of data being obtained and acted upon in good faith by the public authority. The Home Office is therefore considering revising the definition of relevant error in the CD CoP to clarify the point at which errors occur and the actions required to be taken by a public authority or a TO. We currently seek to investigate errors of either origin. However, the absence of provisions for TO errors under section 231(1) of the IPA means that the IPC will not make a determination in relation to informing a person of a serious error for those errors. An example of this is Error Investigation 10 in Annex C.

Definition: determination

A determination usually implies the conclusion of a dispute by the rendering of a final decision.

Reportable and recordable errors

- 18.27 There are two categories of error for CD: recordable and reportable (see paragraphs 18.11 and 12.48 respectively). Errors can occur when an approved application for targeted CD is initiated, or a notice served on a TO, which results in the acquisition of incorrect data or would have resulted in incorrect data if it had not been identified. We expect the authorities we oversee to be tracking both types of error to identify and rectify common themes and prevent future mistakes. The appropriate Senior Responsible Officer (SRO) must have sight of error reports to enable any necessary strategic changes to policy or procedures. There is no obligation for authorities to notify the IPC of recordable errors and so these are not tracked in our annual statistics.
- 18.28 In 2019, 1,063 CD errors were reported to the Commissioner by authorities we oversee (see tables 4 and 5 and Figure 27). We investigated each error and re-categorised 52 of those as recordable, making a total of 1,011 reportable errors. This is an overall increase of 108 errors over 2018, or nearly 12%. Looking further, the detail shows that whilst the number of errors reported by law enforcement and public authorities has remained steady, there has been a marked increase (103) in the number of TO errors.
- 18.29 There is an ever increasing need to acquire CD from overseas TOs. In 2018 the number of reportable errors emanating from overseas TOs was 25, but in 2019 this number had risen to 72. In 38 of these cases incorrect data (16) or data for the wrong period (22) was supplied. Errors emanating from overseas TO data led to three serious error investigations (Annex C, cases 10, 13 and 14).
- 18.30 The NCA has well established links with TOs and can therefore react to issues of data quality. As requests to overseas TOs grow, it is the responsibility of every investigator and single point of contact (SPoC) to check and challenge the data that they are supplied. In 2019 this check and challenge process led to the NCA approaching two overseas TOs. In subsequent meetings with IPCO and the Knowledge Engagement Team (KET) who provide guidance and support from the Home Office for the CD SPoC Community, briefings were produced for the benefit of all relevant public authorities. The ability to react quickly in both cases meant that no serious errors occurred, which was a most welcome outcome.

Reportable errors

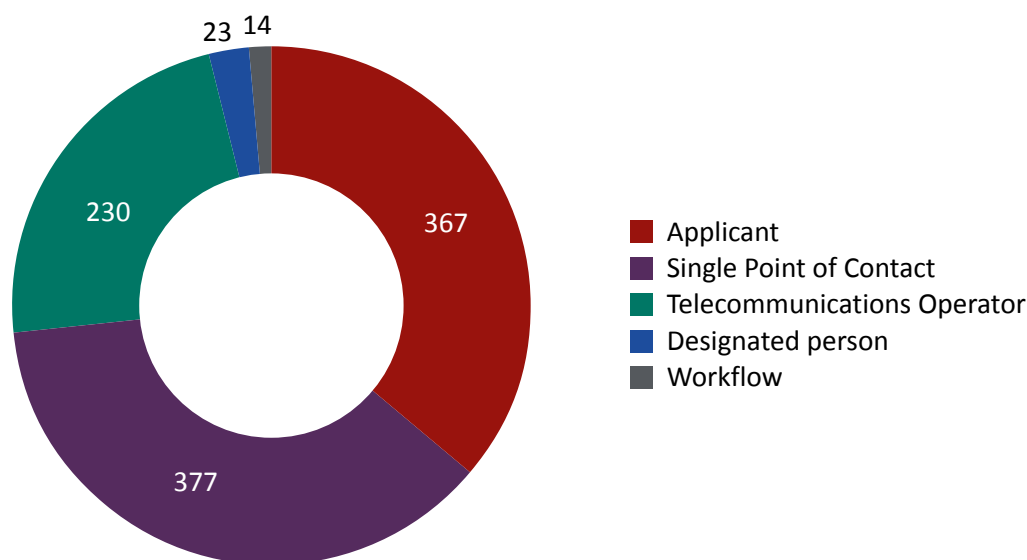
18.31 The majority of CD errors reported by law enforcement agencies and public bodies continue to relate to the actions of a SPoC or the applicant (74%), as shown by the tables below. This is consistent with the reported errors for 2018 and is broadly proportionate to the roles these individuals play in handling CD applications and data.

Table 4: Reportable communications data errors in 2018 and 2019

Cause of error	Number of errors	
	2018	2019
Law Enforcement Agencies	758	755
Telecommunications Operator	127 ⁵⁸	230
Workflow (Other 2018)	13	14
Other Public Authorities	5 ⁵⁹	12
Total	903	1011*

*Six errors were identified during IPCO inspections and subsequently reported.

Figure 27: Communications data errors by responsible authority or system, 2019



18.32 As shown by the following breakdown, the biggest single cause of an error rests with the applicant seeking CD upon an incorrect identifier (telephone number, username, email address or internet protocol (IP) address). Equating to over 30% of all LEA errors, the causes are many and varied with the overall percentage of Internet Protocol Address Resolution (IPAR) errors remaining unchanged when compared to 2018.

58 Last year this figure was shown as 126 in 2018 – one error has been re-categorised.

59 This figure was shown as 6 in 2018 – one error has been re-categorised.

Table 5: Breakdown of communications data errors by error type and responsibility, 2019

	Applicant	Single Point of Contact	Telecoms Operator	Designated Senior Officer	Workflow
Incorrect Identifier	312 (26 IP)	69 (10 IP)	52		
Time Date	40 (11 IP)	170 (62 IP)	93		
Data Type	9	134	56		
Excess/No Data			18		
System Error			4		14
No Authority			4	21	
Other	6	4	3	2	
Total	367 (37 IP)	377 (72 IP)	230	23	14

Reportable errors – Applicant

- 18.33 286 errors were made by applicants when transcribing a telephone number. Officers tend to hand type the number into an application as the number itself is seldom capable of being electronically copied over. In 46 of these reports, the error emanated from victims, witnesses or family members providing officers with the wrong number.

Reportable errors – Single point of contact (SPoC)

- 18.34 The 377 (37%) errors made by a SPoC remains a reflection of their central role in the acquisition of all CD. Applications made within an authority's own workflow system will often require data to be transferred. The identifier, date and time and data type must be entered by the SPoC into a variety of different online TO disclosure systems. This is where all but four SPoC errors occurred.
- 18.35 We welcome any opportunity to use technology to eliminate the manual transfer of data. Developed by the Home Office, automatic acquisition (AA) was introduced in 2019. This process allows an authority's workflow system to send an authorised request electronically to a TO without the need for SPoCs manually to type the requested data into another system.
- 18.36 We expect that the move to AA will continue to bring a decline in transposition errors. However, of the 100 relevant authorities who acquire the most CD, just 31 use AA. At the 31 authorities who can, nearly 80% of all acquisitions are through AA. We expect the remaining authorities to implement this capability over the coming year.

Reportable errors – Telecommunications Operators (TOs)

- 18.37 We work closely with TOs whenever an error is identified to determine the cause and impact of the issue. The number of errors made by TOs has increased by 80% over 2018 to 230. Whilst this is a significant increase it is not large (0.03%) in the context of the approximately 750,000 items of targeted data acquired. Of the 230 TO reported errors, we classified just six as serious; four of these were the result of technical issues and two the result of human error. Nonetheless, we continue to encourage TOs to develop and implement processes to minimise errors as far as possible.

Serious error investigations

18.38 We investigate all relevant errors (see para 18.11 for further information) that are reported to us which we judge may fall within the definition of a serious error as set out in the IPA. Circumstances which we judge to be potentially serious remain:

- i. technical errors relating to the communications service provider (CSP) secure-disclosure systems which result in a significant number of erroneous disclosures;
- ii. errors when a public authority has initiated a course of action that has an adverse impact on someone (for example, sharing information with another public authority stating a person is suspected of a crime; when an individual is visited, or a search warrant is executed; or there is an arrest); and
- iii. errors which result in the wrongful disclosure of a large volume of CD or a particularly sensitive data set.

18.39 We undertook 18 serious-error investigations in 2019 and determined that 14 cases were serious errors, namely where an instance of non-compliance has resulted in significant prejudice or harm to an individual or individuals. The IPC has a duty to inform affected parties of a serious error under section 231 of the IPA, if he judges that this is in the public interest. These cases are summarised at Annex C.

Table 6: Serious errors by cause, 2019

Error Type	Applicant	Single Point of Contact	Telecoms Operator
Identifier	3	1* (2 IP)	1
Time Date		1 (1 IP)	
Data			4
Misinterpretation – Identifier		2 (1 IP)	
Misinterpretation – Data	1		1 (1 IP)
Total	4	4	6

**Error 1 – two different addresses visited.*

18.40 The IPC judged that significant harm was clearly apparent in four of the 14 cases where we made a determination. This number has fallen from eight in 2018. Three of these cases involved the upload of indecent images and the fourth was a crime in action. Common to all was the need to resolve the customers allocated to an IP address at a specified time and date. As shown at Annex C, in two of those cases, the IPC wrote to the affected person(s) informing them of their rights to apply to the Investigatory Powers Tribunal (IPT) if they wished to do so.

18.41 As noted at paragraph 18.26, our serious error investigations included errors relating to TOs. In three investigations the definition of 'relevant error' was not met because the error was made by a TO, not a public authority. In two of these cases, we judged that significant harm to a person had occurred, but no determination could be made. However, it is possible that the operation of data protection legislation may result in a notification to the affected party of the error. We have not, therefore, informed any individuals of harm which we believe to have met this threshold.

18.42 Errors made on the identifier or the time and date of IP usage pose the greatest risk of a serious error. Out of the 1,011 reportable errors, 506 fell into this high-risk category. Of

the 14 investigations appearing in Annex C, 10 were from this high-risk category. We are therefore pleased to report that the other 496 errors in this area were all discovered before any potentially harmful action was taken.

- 18.43 The discovery of these errors at an early stage can be largely attributed to the Error Reduction Strategy (ERS) produced by the National Police Chiefs Council (NPCC) – Data Communications Group in consultation with IPCO. Throughout 2019, we inspected compliance with the ERS, focusing on the three key peer review stages:

- i. accuracy of identifier(s) in the application matched identifier(s) in any source document;
- ii. validating the accuracy of the identifiers entered into a TO disclosure system*; and
- iii. confirming the identifier(s) in the result match those in the application and or source document.

**Step eliminated if AA is used (See paras 18.35 and 18.36).*

- 18.44 We found that good audit processes were evidenced. Anomalies identified during peer review (stage i.) are recorded as 'near misses' as no formal reporting to IPCO is required prior to the application being authorised. Recording 'near misses' acts as an indicator, to the SRO and to our Inspectors, of SPoC staff adhering to the ERS.
- 18.45 Table 6 shows that the greatest number of major errors were caused by TOs. Those involving erroneous data from a TO are the most difficult to detect. We continue to encourage LEAs to mitigate against such errors through corroboration. Uncorroborated internet-based CD should only be used as the sole basis for action on an exceptional basis.
- 18.46 The misinterpretation of data was the reason behind four of the investigations found in Annex C. In three, the results led to certain assumptions that later proved to be incorrect. In the fourth, open source research identified the wrong social media account of the person sought. The misinterpretation of accurately acquired data represents a shift in causation away from the simple transposition errors.
- 18.47 Because of the large number of applicants and SPoCs, and the potential for similar errors to be made at different organisations, we believe that the community should be taking opportunities to learn and make improvements based on the mistakes of others. We have therefore encouraged the practice of briefing any errors of data misinterpretation, or errors of a technical nature, to the SPoC community as soon as possible. This means that the community can assess potential risk at a local level and implement interim solutions, where necessary. We have found that the level of engagement shown by the Home Office's Knowledge Engagement Team and National Communications Data Services Unit, and the TOs, is crucial to the success of this work and we expect this community to continue to meet regularly to discuss errors, risks and improvement strategies in line with the National Error Reduction Strategy for IPAR.

19. Statistics

Overview

- 19.1 We collect a range of statistics to inform our understanding of how investigatory powers are being used across the country. This is a complex and time-consuming exercise each year, both for the Investigatory Powers Commissioner's Office (IPCO) and for the organisations we oversee. We are in the process of reviewing the way we collect information and hope that we will shortly be able to introduce changes which both streamline the process and ensure that the information we produce is as reliable as it can be.
- 19.2 We have selected statistics for publication which we believe will give an accurate picture of the extent to which the different categories of authority that we oversee are using their powers, and to which specific powers are used. The context within which they are being used, and our findings from recent oversight, are given in the previous chapters. Where possible, we have sought to present statistics in the same format as our previous report to enable comparisons to be drawn, however, the authorities we oversee continue to be in a period of transition which means that in some cases statistics will not present a like-for-like comparison.
- 19.3 As we have noted in other chapters, we are challenged every year on the value of the statistics we publish. We welcome this challenge, which will help us continue to improve the level of transparency we offer to Parliament and the public through our report. As an organisation, we are committed to ensuring that we do not provide statistics which would be partial or misleading, as well as those which could cause any damage to the ongoing operations of the authorities we oversee and to national security. For this reason, we provide limited statistics in relation to the functions of the intelligence agencies, where we would not be able to give sufficient contextual detail to enable those figures to be analysed effectively by readers. It is also worth noting here that while we do collect statistics, we do not take a structured or statistically-driven approach to oversight, which we believe is best conducted on the basis of compliance risk and areas of clear public interest.
- 19.4 With this in mind, this chapter provides statistics on the use of covert powers by the authorities we oversee, including those required to be published in this report under section 234⁶⁰ of the Investigatory Powers Act 2016 (IPA).
- 19.5 Due to the impact of COVID-19, IPCO had not received statistical returns from ten local authorities and one wider public authority by 30 June 2020. These authorities are all low users of investigatory powers and analysis of their returns for 2018 shows that their exclusion from this year's statistics will not have a material effect on their accuracy.

60 Section 234 of the Investigatory Powers Act 2016 requests the publication of key statistics, including the number of warrants and authorisations issued, given, considered and approved during the year.

Warrants and authorisations

- 19.6 The following table gives total numbers for the warrants and authorisations issued, given, considered and approved for the period 1 January 2019 to 31 December 2019. It also provides the total number of certain notifications made to IPCO during this period.
- 19.7 In our 2018 report, we did not include figures for the number of warrants and authorisations considered, in addition to those granted, where there was a period of transition in relation to that power. For example, targeted interception was only subject to judicial consideration in the latter half of 2018 and so we did not identify how many warrant applications had been considered during that period. This was omitted to prevent providing misleading partial statistics. We have taken the same approach in the table below for any powers that transitioned during 2019. However, we are now able to give a fuller picture of the work done by IPCO and the Office for Communications Data Authorisations (OCDA), as set out below. As noted in previous chapters, any application that has not been granted after consideration will have been refused or withdrawn. This could have been the result of judicial challenge or to changes in the planned operation by the requesting agency.

Table 7: Breakdown of authorisations, including those considered by a Judicial Commissioner, 2019

	Considered by a Judicial Commissioner	Approved, issued or given	Refused by a Judicial Commissioner
Covert human intelligence sources (CHIS) including juveniles	–	3,652	NA
Directed Surveillance	–	8,049	NA
Intrusive Surveillance	–	533	2
Property Interference under the Intelligence Services Act section 5	–	497	NA
Property Interference under the Police Act 1997	999	999	0
Bulk personal datasets – class warrant	101	101	0
Bulk personal datasets – specific warrant	85	85	0
Directions under section 219 of the Investigatory Powers Act	0	0	0
Directions under section 225 of the Investigatory Powers Act	7	7	0
Bulk communications data acquisition warrant	18	18	0
Communications data authorisation	–	200,665	NA
Bulk interception warrant	30	30	0
Targeted examination of interception warrant	49	49	0
Targeted interception warrant	3,330	3,329	1
Bulk equipment interference warrant	10	10	0
Targeted examination of equipment interference warrant	43	43	0
Mutual assistance warrant	0	0	0
Targeted equipment interference warrant	1,931	1,919	17
Relevant source notification	–	752	5
Request to retain legal professional privileged material	98	97	1
Notification under section 77 of the Investigatory Powers Act	17	17	0

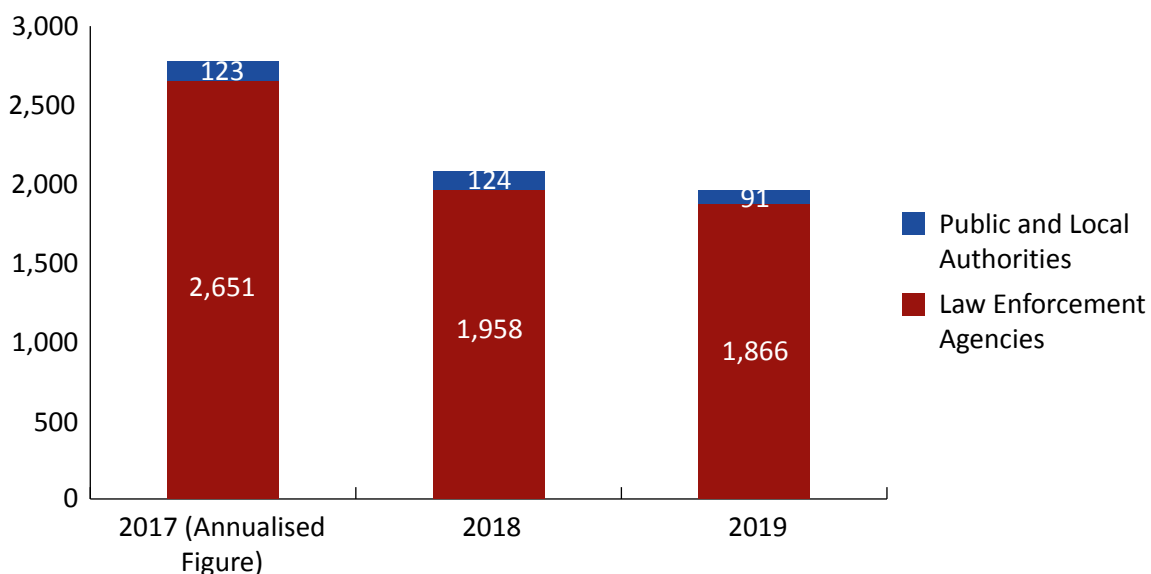
Breakdown of the use of powers throughout 2019

19.8 The charts included in this chapter are intended to demonstrate trends in the use of investigatory powers across the authorities we oversee. These charts have been produced to enable year-on-year comparison.

Covert human intelligence sources (CHIS)

19.9 Our predecessor organisation (the Office of Surveillance Commissioners) tracked the use of CHIS by law enforcement, local authorities and public authorities over the past decade. There has been a steady decline in the use of CHIS which we believe reflects the changing shape of investigations and the commitment by forces to use the most appropriate and least intrusive method of investigation. Whilst the number of CHIS authorisations fell slightly in 2019, we expect the number of authorisations for CHIS to remain around the current level over the coming years.

Figure 28: Covert human intelligence sources of law enforcement agencies, public and local authorities, 2017 – 2019⁶¹



Relevant sources

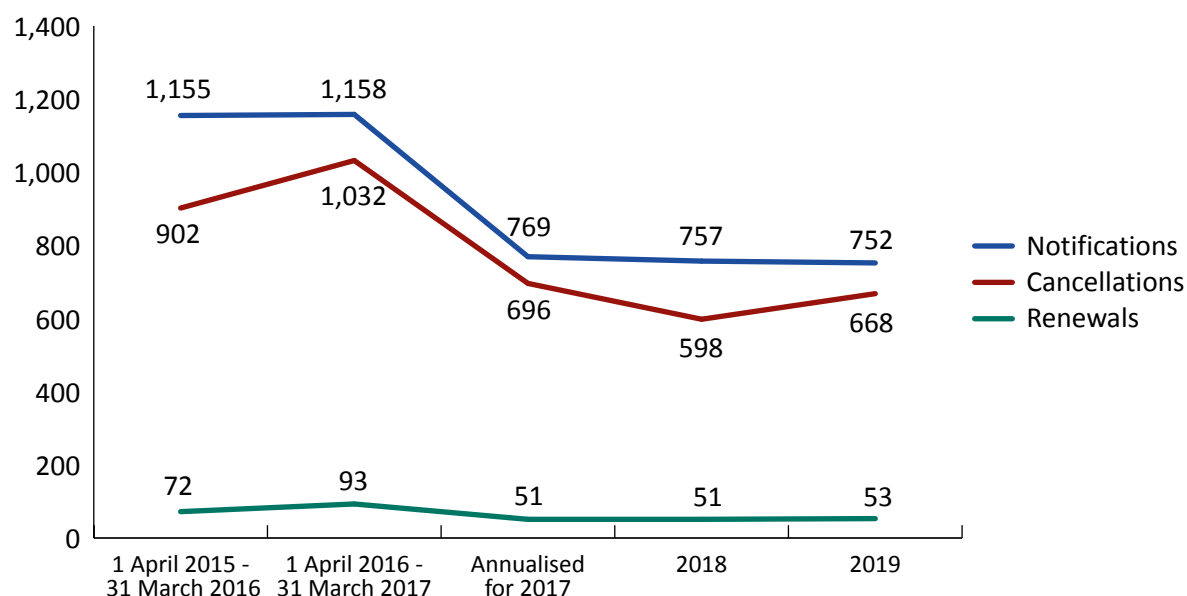
19.10 Undercover officers are known legally as relevant sources⁶² and applications are authorised within the force or public authority for 12 months. A renewal must be authorised by a Judicial Commissioner (JC). At the nine-month point, the authority must notify the Investigatory Powers Commissioner (IPC) of their intention to renew that authorisation if and when it reaches the 12-month point; upon this notification one of our Inspectors will carry out a review of the operation to date and their report will be available both to the Authorising Officer (AO) and the JC. Such notification is not a guarantee that the authority will still actually seek to renew but, if they choose not to, then the authorisation must be cancelled. We continue to see that most authorisations are cancelled within the first year.

61 Note that the key on this table in the 2018 Annual Report is mis-coloured such that the graph misleadingly suggests that a high number of applications were made by public and local authorities.

62 As defined by the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013.

In 2019 we conducted 47 inspections for the renewal of relevant source authorisations with respect to 87 relevant sources.

Figure 29: Relevant sources, 2015 – 2019 notifications, cancellations and renewals⁶³



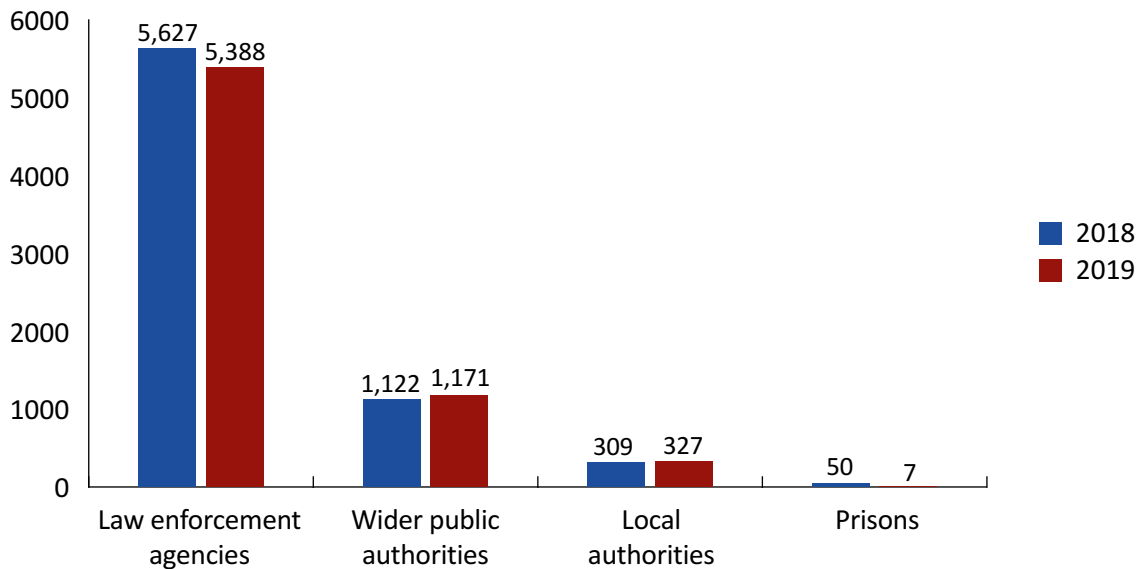
Directed surveillance

19.11 As noted in the previous chapters, directed surveillance is a critical investigative tactic for the range of authorities that we oversee and is available to public and local authorities as well as law enforcement. Directed surveillance has evolved in recent years to include online tactics as well as traditional physical surveillance methods. There has been a slight fall in the overall number of directed surveillance authorisations (DSAs) over the last year.⁶⁴

⁶³ Note that this figure was given incorrectly in Table 6 of our 2018 Annual Report. In 2018, 757 relevant source applications were granted, 51 were renewed and 598 were cancelled.

⁶⁴ Note that these figures were given incorrectly in our 2018 Annual Report. In 2018, Law enforcement and Police were granted 5,627 directed surveillance authorisations, wider public authorities were granted 1,122, Prisons were granted 50, local authorities were granted 309 and the Ministry of Defence was granted 40 authorisations.

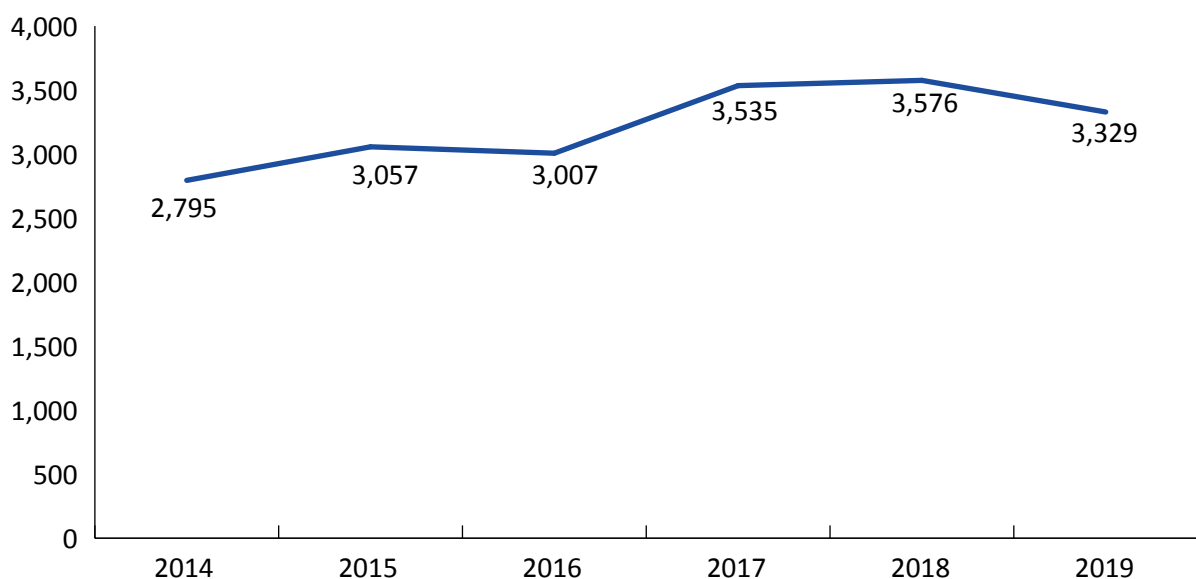
Figure 30: Directed surveillance across law enforcement agencies and wider public and local authorities⁶⁵



Targeted Interception

19.12 The number of targeted interception (TI) authorisations has been relatively steady over the last three years with a slight reduction in 2019. For the UK Intelligence Community (UKIC) many TI warrants were combined with targeted equipment interference (TEI). TI applications made in combined warrants are shown in the total figure below. The percentage of urgent applications has fallen to around 3%, which is lower than in previous years.

Figure 31: Targeted interception authorisations by the UK Intelligence Community, the Ministry of Defence and law enforcement agencies, 2014 – 2019.

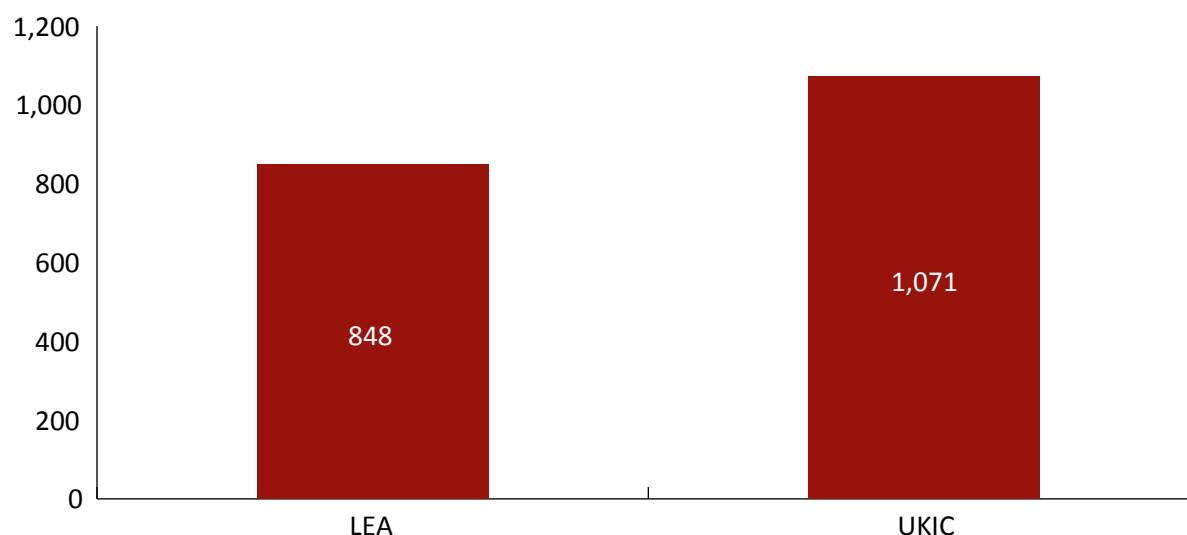


⁶⁵ Fire and Rescue Services appeared as a nil return in this table in last year's report. They no longer use directed surveillance powers and will in due course be removed from the schedule of public authorities authorised to do so.

Targeted equipment interference (TEI)

- 19.13 The number of targeted equipment interference (TEI) authorisations cannot be presented as comparable statistics because the introduction of TEI warrants under the IPA established a new category of authorisation for activity which was previously conducted under disparate legislation. Because 2018 was a period of transition, the total of TEI warrants authorised will not reflect the total number of warrants that would have been approved within the year if the regime had been in place. In other words, some warrants that would now be TEI warrants will have been property interference warrants under the Police Act 1997 or Intelligence Services Act (ISA) 1994. Therefore, the figure below shows 2019 authorisations only and for UKIC includes applications made under combined warrants.

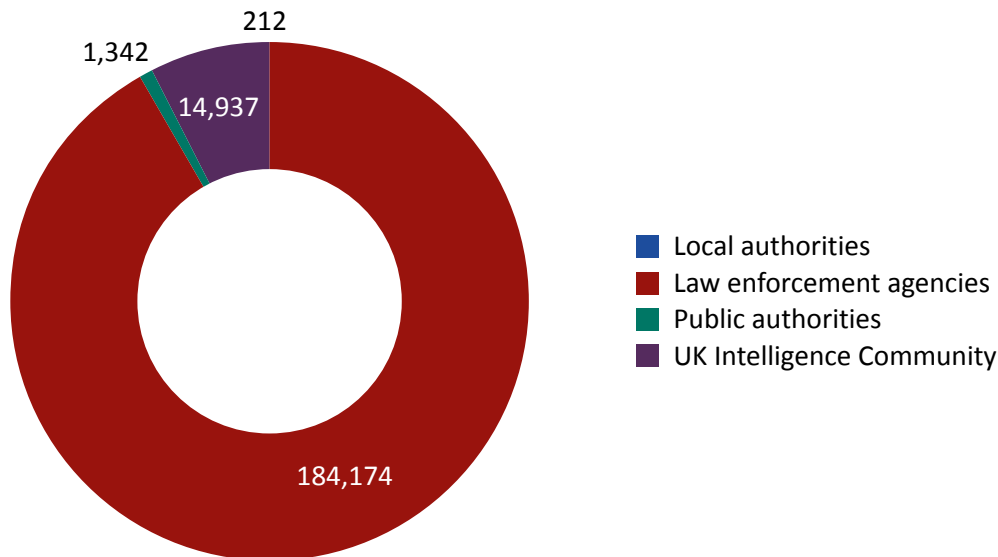
Figure 32: Targeted equipment interference authorisations for the UK Intelligence Community and law enforcement agencies, 2019



Targeted communications data (CD)

- 19.14 As in our 2018 report, we have given a breakdown of the use of communications data in the chapters covering law enforcement, local authorities and public authorities. A total of 200,665 requests to obtain communications data were approved in 2019, including UKIC. Communications data requests continue to be the most voluminous of the authorisations for covert powers. As in previous years, the greatest number of applications were made by law enforcement. A full break down of approved CD requests by organisation is also given in Annex D.
- 19.15 As shown in the previous chapters, CD applications are used to request one or more data items. Unfortunately, the systems used to process that data are not able to provide precise statistics and we believe that there is a margin of error of around 10% on the number of data items obtained. However, the nature of our oversight means that this does not reduce the level of confidence that we have in the compliance of those authorities. In the region of three quarters of a million CD items were obtained in 2019.

Figure 33: Targeted communications data authorisations granted by type of organisation



Office for Communications Data Authorisations (OCDA)

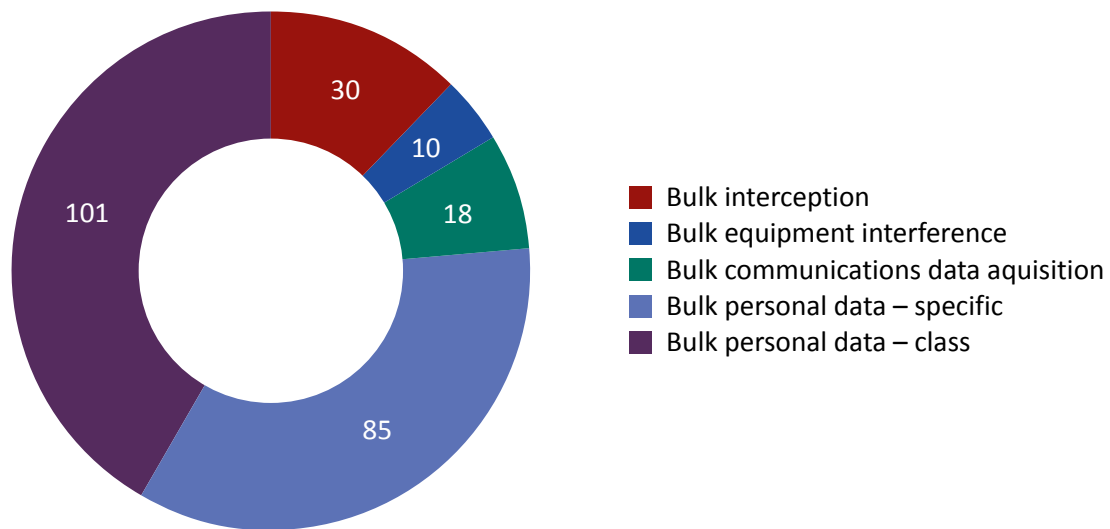
- 19.16 The introduction of OCDA to review and approve CD requests means that CD statistics will be more accurate in the future. As set out in chapter 5, OCDA takes a decision on all routine and priority CD requests, but not urgent applications. This applies to all authorities obtaining CD, with the exception of UKIC.
- 19.17 OCDA took its first decision on a CD application on 26 April 2019. The following table shows how many decisions on applications were taken by OCDA in the period to 31 December 2019.

Table 8: Communications data applications received by the Office for Communications Data Authorisations in 2019

Applications received	71,610
Decisions made	71,208
Authorised	63,688
Not authorised	7,520
Withdrawn	385
Applications with no decision (e.g. pending as at 31 December)	17

Bulk Powers

- 19.18 While the underlying capabilities are not new, the IPA introduced specific warrants for bulk collection powers. Bulk warrants are often long standing so the number of applications for new warrants is not a good measure of the level of activity. The chart below shows the number of new applications and renewals for each class of bulk warrant for 2019. Figure 28 in the 2018 report related only to new authorisations.

Figure 34: Bulk warrants and renewals by type⁶⁶

Consolidated Guidance

- 19.19 In our 2018 Annual Report, we set out the difficulties associated with publishing clear, reliable statistics about UKIC/MOD's use of the Consolidated Guidance. Many of the problems highlighted in our previous report persist: for instance, it is not possible to publish a reliable figure on the number of times the Consolidated Guidance was considered by UKIC/MOD because of the way in which records are maintained by them and the associated risk of "double counting". As we noted in our 2018 report, the available statistics cover the number of times administrative processes relating to the internal policies for applying the Consolidated Guidance had been exercised, not the number of cases engaging the Consolidated Guidance which had been considered.
- 19.20 However, we have now identified a set of statistics which give some sense of UKIC/MOD's use of the Consolidated Guidance in practice. The table below sets out the total number of cases in which UKIC/MOD referred to Ministers for a decision because there was a serious risk of one of the categories of mistreatment (torture, for example) set out in the Consolidated Guidance. They also include the number of cases which UKIC/MOD proactively brought to our attention because they raised particular legal or policy issues – some of which have informed the findings presented in this report.
- 19.21 There are important caveats to the data presented here. First, an increase in cases which cross the threshold of serious risk (in the Consolidated Guidance) or real risk (in The Principles) does not, necessarily, indicate that UKIC/MOD have taken additional risks in their engagement with overseas authorities. A single operation (such as, in response to a major terrorist plot) may generate a "spike" in referrals to Ministers, for example. As such, it will not be possible to conduct a straightforward year on year analysis of these figures to determine whether or not the overall level of risk associated with the application of the Consolidated Guidance has increased. Similarly, a reduction in the number of cases does not necessarily suggest a lower risk appetite has been adopted.
- 19.22 Second, as the Consolidated Guidance makes clear, consulting Ministers does not imply that action will or will not be authorised, and the UK Government's clear stated policy is that the

⁶⁶ This figure was given incorrectly in our 2018 Annual Report. Three warrants for bulk equipment interference were authorised in 2018.

UK does not participate in, solicit, encourage or condone unlawful killing, the use of torture or cruel, inhuman or degrading treatment, or extraordinary rendition.

- 19.23 Third, there is a small risk of “double counting” in these figures: the same case could have been referred to Ministers by more than one agency or department. However, following the implementation of The Principles in January 2020, all of the relevant agencies and departments have now agreed that the last organisation to handle intelligence before it is handed to an overseas authority will take responsibility for completing a Principles assessment on behalf of any others who may be involved. This will tend to reduce the likelihood of “double counting” in future years.

Table 9: Consolidated Guidance, the UK Intelligence Community and the Ministry of Defence

Number of cases reviewed on inspection		56
Number of cases brought proactively to the attention of the Investigatory Powers Commissioner's Office because they posed contentious legal or policy issues		10
Total number of all Consolidated Guidance cases (not limited to those reviewed on inspection), across all Consolidated Guidance public authorities, where personnel:	Knew or believed torture would occur	0
	Identified a serious risk of torture and submitted for approval despite the presumption not to proceed in such cases	2
	Identified a serious risk of cruel, inhuman or degrading treatment and submitted for approval	7
	Identified a serious risk of lack of due process and submitted for approval ⁶⁷	21

67 This is a shorthand for standards of arrest and detention under a) and b) of the Annex to the Consolidated Guidance, namely the lawfulness of the arrest (under local law) and the lawfulness of the detention (under local and international law) and access to due process.

Annex A: Glossary of Authorities

The following table sets out the authorities we oversee. There have been no changes to the authorities we oversee since the introduction of the Investigatory Powers Act (IPA).

Intelligence Agencies	<ul style="list-style-type: none"> • Secret Intelligence Service (SIS) • Security Service (MI5) • Government Communications Headquarters (GCHQ) <p>References to 'UKIC' mean the United Kingdom Intelligence Community.</p>
Defence	Ministry of Defence
Law Enforcement Agencies (LEAs)	<ul style="list-style-type: none"> • All territorial police forces in the UK • All other police forces including the British Transport Police, Ministry of Defence Police, Royal Military Police, Royal Air Force Police, Royal Navy Police, Civil Nuclear Constabulary, Port of Dover Police, Port of Liverpool Police • Her Majesty's Revenue and Customs (HMRC) • National Crime Agency (NCA) • The Home Office (Border Force and Immigration Enforcement)
Wider Public Authorities (WPAs)	<ul style="list-style-type: none"> • British Broadcasting Corporation (BBC) • Care Quality Commission • Centre for Environment, Fisheries and Aquaculture Science (CEFAS) • Charity Commission • Competition and Markets Authority • Criminal Cases Review Commission • Department for Business Innovation and Skills (Insolvency Service) • Ministry for Housing, Communities and Local Government (MHCLG) • Department for Work and Pensions (DWP) • Department for the Economy for Northern Ireland • Department for the Environment, Food and Rural Affairs (DEFRA) • Department for Transport – Air Accident Investigation Branch (AAIB) • Department for Transport – Driver and Vehicle Standards Agency (DVSA) • Department for Transport – Marine Accident Investigation Branch (MAIB) • Department for Transport – Maritime and Coastguard Agency (MCA)

Wider Public Authorities (WPAs) <i>continued</i>	<ul style="list-style-type: none"> • Department for Transport – Rail Accident Investigation Branch (RAIB) • Environment Agency • Financial Conduct Authority (FCA) • Food Standards Agency • Food Standards Scotland • Gambling Commission • Gangmasters and Labour Abuse Authority (GLAA) • General Pharmaceutical Council • Health and Safety Executive • Health and Social Care Northern Ireland • Her Majesty's Chief Inspector of Education, Children's Services and Skills (OFSTED) • Her Majesty's Prison and Probation Service (HMPPS) • Independent Office for Police Conduct (IOPC) • Information Commissioner's Office (ICO) • Marine Scotland • Maritime Management Organisation • Medicines and Healthcare Products Regulatory Agency • National Anti-Fraud Network (NAFN) • National Health Service (NHS) Business Services Authority • National Health Service (NHS) Counter Fraud Authority • Natural Resources Wales • Northern Ireland Office (Prison Service for Northern Ireland) • Office of Communications (Ofcom) • Office of the Police Ombudsman for Northern Ireland (PONI) • Police Investigations and Review Commissioner (PIRC) • Prudential Regulation Authority • Royal Mail • Scottish Accountant in Bankruptcy • Scottish Criminal Cases Review Commission • Scottish Environmental Protection Agency (SEPA) • Scottish Prison Service • Serious Fraud Office • Social Security Scotland • The Pensions Regulator • Transport Scotland • Welsh Assembly Government
Local Authorities	All UK local authorities
Prisons	All prisons in England, Wales, Scotland and Northern Ireland
Fire and Rescue Services	All separately constituted Fire and Rescue services in the UK
Ambulance Services	All UK Ambulance Services

Annex B: Budget

This table gives a breakdown of the Investigatory Powers Commissioner's Office's (IPCO) and the Office for Communications Data Authorisations (OCDA) financial statements for the financial year for 2019/2020.

IPCO Budget breakdown – Annual Year 01/04/2019 – 31/03/2020		
	19/20 Full Year Budget Allocation	19/20 Full Year End Outturn
Pay Costs	£4,613,550	£4,542,807
Estates	£520,000	£850,533
IT & Comms (+ Marketing)	£67,459	£178,825
Travel & Subsistence	£750,000	£349,028
Other Costs & Services (TAP)	£260,000	£76,728
Training & Recruitment (+ conferences)	£50,000	£12,617
Office Supplies & Services	£40,000	£13,836
Consultancy	£100,000	£12,293
Total	£6,401,009	£6,036,667

OCDA Budget breakdown – Annual Year 01/04/2019 – 31/03/2020		
OCDA Budget Detail	19/20 Full Year Budget Allocation	19/20 Full Year End Outturn
Pay Costs	£5,100,000	£4,279,202
Estates	£500,000	£530,118
IT & Comms (+ Marketing)	£1,300,000	£1,116,896
Travel & Subsistence		£131,642
Consultancy (legal)		£90,285
Training & Recruitment (+ conferences)	£100,000	£42,995
Office Supplies & Services		£32,897
Capital Costs	£1,600,000	£115,441
Total	£8,600,000	£6,339,477

Annex C: Serious Errors

The Investigatory Powers Commissioner (IPC) decided that the following errors amounted to a serious error within the meaning of section 231 of the Investigatory Powers Act 2016 (IPA). Further details on serious errors are given in chapter 18 and on our website [www.ipco.org.uk]. As noted in chapter 18 our investigations have included potential errors made by Telecommunications Operators (TOs).

Error Investigation 1

	Public Authority
Human or Technical:	Human, single point of contact (SPoC)
Classification:	Transposition
Data Acquired:	Customer information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A public authority had arrested a suspect for online grooming offences. The online activity had been conducted using different internet protocol (IP) addresses and so the officers worked to confirm that the assigned broadband customer for these IP addresses was the suspect. The public authority made a series of requests to establish the customer assigned use of the IP addresses. Two errors were made during acquisition;</p> <ol style="list-style-type: none"> the last three digits from another IP address relating to the same investigation was used when the request was sent to the provider; and to ensure the correct customer was identified, the IP's session time was requested by the authority. This brought back the email addresses for two customers (the suspect and a previous customer who had been allocated the IP address in the past). The public authority made a request against the wrong email address, which produced the name and address of the previous customer.
Consequence:	<p>Two homes unconnected to this investigation were visited and the occupants spoken to.</p> <p>There was no determination by the IPC, as the effect on those visited was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 2

	Public Authority
Human or Technical:	Human (Applicant)
Classification:	Transposition
Data Acquired:	Subscriber information relating to an email address and recent IP logon history.
Description:	<p>A police authority was trying to locate an individual because of concerns for their welfare. An officer identified the individual's email address. They sought, via the SPoC, to resolve when and where the person had last used their email account. The officer was unable to cut and paste the email address into the incident log and so manually transposed it. When doing so, they mistyped the email address.</p> <p>A request was made on an incorrect email address and the provider returned details of the account's most recent activity. Officers were deployed to locate the user of that account to check on their welfare. Once they realised their mistake, the officers replicated the search on the correct account and found it to be inactive.</p>
Consequence:	<p>Police visited the premise of an individual unconnected to their search. There was no determination by the IPC, as the effect on those visited was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 3

	Public Authority
Human or Technical:	Human
Classification:	Transposition
Data Acquired:	Subscriber information relating to a telephone number.
Description:	<p>A police force was trying to locate an individual due to concern for their welfare. The authority had previously conducted checks on the individual for similar reasons. The authority's records included a contact number for the individual.</p> <p>The authority submitted checks to confirm the subscriber to the number and visited the address listed on the account. Its owner, who was able to produce the phone, clearly had no connection to this enquiry. A check of the previous record ascertained the recorded number had been entered into the system incorrectly.</p> <p>Once this had been rectified, the authority was able to locate the individual, who was found to be safe and well.</p>
Consequence:	<p>Police visited the premise of an individual unconnected to their search. There was no determination by the IPC, as the effect on those visited was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 4

	Public Authority
Human or Technical:	Human (SPoC)
Classification:	Misinterpretation of Data
Data Acquired:	Username activity: Customer information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A public authority had arrested a suspect for online grooming offences. Following pre-charge advice, an officer made an application to identify where the suspect's username had accessed the internet.</p> <p>The IP address covering the time and date was supplied to the public authority by the overseas TO. The document provided by the TO consisted of two pages with the IP address located on page one.</p> <p>The SPoC resolved the IP address and obtained customer details, including a name and address for the suspect. The authority made a visit to the address. The visit found no family link to the suspect and the officers suspected that an error had been made.</p> <p>Closer examination of the overseas result revealed on page two a declaration stating the last octet for the IP address had, for GDPR reasons, been truncated to a zero.</p> <p>For this particular IP, the last octet could be any number between 0 – 265. The TO had changed each of the 265 endings all to a zero.</p>
Consequence:	<p>A home of a family unconnected to this investigation was visited and the occupants spoken to.</p> <p>There was no determination by the IPC, as the effect on those visited was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 5

	Public Authority
Human or Technical:	Human (Applicant)
Classification:	Misinterpretation of open source research.
Data Acquired:	Recent log on activity for a social media account.
Description:	<p>A police force was trying to locate and arrest a person wanted in connection with serious firearms offences. An officer identified what they believed was the wanted person's Facebook profile and used a communications data request to identify an address associated with the active profile. Officers visited this address, which had been shown to be associated with recent activity on the account.</p> <p>Upon arrival, officers established the person living at the address had the same name as the suspect but no link to the crime under investigation. The Police subsequently identified that the two profiles were identical in name but with a different numerical suffix.</p>
Consequence:	<p>Police visited the premise of an individual unconnected to their search. There was no determination by the IPC, as the effect on those visited was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 6

	Public Authority
Human or Technical:	Human (SPoC)
Classification:	Transposition
Data Acquired:	Customer information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A public authority was investigating the uploading and sharing of indecent images of children (IIOC). The officer identified the IP address involved and applied for details of the customer assigned this IP at the time of the upload.</p> <p>When obtaining the data from the portal, the SPoC erroneously selected 2019, rather than 2018, as the timestamp for the request. The SPoC gave the resulting, incorrect customer details to the investigating officer. A warrant was obtained, executed and the innocent customer was arrested, interviewed and released.</p> <p>The next step of the police investigation was forensic examination of internet-enabled devices seized from the suspect. This would allow police to gather evidence linking the individual to the crime. Four months elapsed before forensic examination took place, at which point the police did not identify relevant material on the devices. When nothing incriminating was found, the police reviewed the case against the suspect and identified the error.</p>
Consequence:	The IPC made a determination in accordance with Section 231 of the IPA 2016. The individual was advised of his/her right to refer the matter to the IPT.

Error Investigation 7

	Public Authority
Human or Technical:	Human (Reporting Person/Applicant)
Classification:	Transposition
Data Acquired:	Subscriber information
Description:	<p>A national charity reported concerns for the welfare of a person they had been in text contact with to the Police. The last digit of the telephone number was either passed or taken down incorrectly. The investigating officer sought, via the SPoC, the name and address of the customer of the now incorrect telephone number.</p> <p>Once the error had been realised, the corrected subscriber check led another set of officers to a house where the person was located.</p>
Consequence:	<p>Police visited the premise of individuals unconnected to their search.</p> <p>There was no determination by the IPC, as the effect on those visited was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 8

	Public Authority
Human or Technical:	Technical
Classification:	Misinterpretation of data (Billing Address)
Data Acquired:	Subscriber information relating to an Internet Protocol Address Resolution (IPAR)
Description:	<p>A public authority was investigating the uploading and sharing of indecent images of children (IIOC). The officer/SPoC identified four relevant IP addresses used by the suspect during upload and sought their resolution into customer details. After authorisation, the applicant received the same customer details against each of four IP addresses submitted.</p> <p>An intelligence package was sent to another public authority for immediate action to safeguard any children involved. Officers attended the address and found no child at the house. The sole occupant was arrested and all internet-enabled devices were seized by the police.</p> <p>However, enquiries later that morning established the public authority had received the billing address not the installation address where the activity had taken place. The result provided by the TO gave no indication the name and address was that of the bill payer and not the customer.</p>
Consequence:	The IPC made a determination in accordance with Section 231 IPA 2016. The individual was advised of his right to refer the matter to the IPT.

Error Investigation 9

	Telecommunications Operator (TO)
Human or Technical:	Human (Disclosure Officer)
Classification:	Incorrect Data
Data Acquired:	Subscriber information relating to a telephone number
Description:	<p>A public authority was investigating conspiracy to supply Class A Drugs. A request for the subscriber of a telephone number at a stated date was submitted to a TO. The result included a name and email contact address. Officers sought to call and email the named individual to arrange a visit. The person's response upon contact led officers to suspect an error. The SPoC contacted the TO and a check revealed they had provided the current subscriber and not the subscriber for the period requested.</p>
Consequence:	<p>Contact was made (five times) with a person unconnected to the investigation.</p> <p>There was no determination by the IPC, as the effect on those visited was assessed not to have caused significant prejudice or harm.</p>

Error Investigation 10

	Telecommunications Operator (TO)
Human or Technical:	Technical
Classification:	Incorrect Data
Data Acquired:	Subscriber information relating to an Internet Protocol Address Resolution (IPAR). Subscriber information for an email address.
Description:	<p>A public authority received a National Centre for Missing and Exploited Children (NCMEC)⁶⁸ report which identified that a social media account had been used to upload indecent images of children (IIOC). The report provided details of a UK IP used to upload the indecent images and an associated email address for the social media account.</p> <p>The IP was quickly resolved, but there were delays in the TO providing subscriber details for the email address. Given TO delays, the Police took action based solely on the IPAR. At this point, officers seized one internet-enabled device but did not make an arrest.</p> <p>Four weeks later, details for the subscriber of the email address were returned and it was not the same individual. The Police contacted the subscriber of the email address and confirmed that there was no link with the user of the IPAR.</p> <p>Our investigation found no error on the part of the public authority. Unfortunately, enquiries with NCMEC and the provider of the email address has failed to establish exactly why the IP or the email address became linked to the crime.</p>
Consequence:	Property was seized from an individual unrelated to the investigation. Under Section 231 (9) the IPC is only able to make a determination if the relevant error is made by a public authority. In this case no error was made by the public authority.

68 The National Centre for Missing and Exploited Children is a private, non-profit corporation whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimisation.

Error Investigation 11

	Telecommunications Operator (TO)
Human or Technical:	Technical
Classification:	Shortfall Data
Data Acquired:	Wi-Fi session data
Description:	<p>A system fault led to the disclosure of inaccurate internet session data records relating to devices attached to public Wi-Fi. The fault was identified by the TO after a short period, during which several disclosures had been made in relation to authorised communications data requests. Once the fault had been fixed, the TO re-ran the data requests and confirmed that 78 had been responded to with incorrect data. The relevant forces were informed immediately.</p> <p>The fault led to the following inaccuracies;</p> <ul style="list-style-type: none"> i. incorrect data records were disclosed (4) ii. results were returned which included partially correct data, but included under or over disclosure of relevant data (36) iii. unfortunately, in the largest bracket, any inaccuracy is unknown. Data protection provisions mean that data is deleted by TOs after 12 months. In the remainder of cases, the data had automatically been deleted before the TO could re-run and verify the data. <p>Session data alone was unlikely to identify an individual. Where the data was still available (under 12 months old) the public authorities were able to request the correct data set and 29 re-runs were requested.</p>
Consequence:	The disclosures under i) and ii) did not result in the identification of a suspect. With no comparison possible under iii) no further action was taken.

Error Investigation 12

	Telecommunications Operator (TO)
Human or Technical:	Technical
Classification:	No Data (during a defined period)
Data Acquired:	Subscriber and call data records
Description:	<p>A system fault prevented a TO's portal from providing subscriber details and call data records covering a 6-day period for routine requests. The TO immediately informed the police of this issue and provided the results of urgent requests manually. This meant that the TO was only able to provide data linked to life at immediate risk.</p> <p>A total of 998 requests were identified as having sought data from within the affected six days. The data for each was rerun and made available to the requesting authority within five days.</p>
Consequence:	There was no impact from this delay in providing data.

Error Investigation 13

	Telecommunications Operator (TO)
Human or Technical:	Technical
Classification:	Incorrect Data
Data Acquired:	Subscriber information relating to Internet Protocol Address Resolutions (IPAR).
Description:	<p>A system fault was reported to UK public authorities by an overseas social networking site. The TO assessed that this could mean that results from IP address resolution requests might be incorrect. The TO included a summary of the error in its NCMEC reports to the UK once the fault had been identified.</p> <p>In total nine reports from the TO included potentially incorrect data, which had been passed to public authorities. All of these reports were investigated by the public authorities to verify the contents;</p> <ol style="list-style-type: none"> on four of the reports, other corroborative evidence was obtained, and the original report was believed accurate. Executive action was taken on two with incriminating evidence found. the results presented in three reports were cross-checked with other available data and no action was taken on them in isolation; and two reports were returned to be actioned again by the TO once the fault had been resolved. In both cases, viable leads were identified from the reissued data.
Consequence:	No action was taken without the data having been corroborated or revalidated. The issue was rectified, and correct data provided swiftly so that action could be taken as appropriate.

Error Investigation 14

	Telecommunications Operator (TO)
Human or Technical:	Human
Classification:	Misinterpretation of data
Data Acquired:	Subscriber information relating to Internet Protocol Address Resolutions (IPAR).
Description:	<p>A public authority was investigating a potential kidnap. The authority identified IP activity for an internet-enabled device linked to the victim. An overseas TO confirmed to the authority that this activity had occurred post kidnap and so the authority requested that the IP address should be resolved to the assigned customer, giving the police an address on which to focus their investigation.</p> <p>Police forced entry to the address. On speaking to the occupant, it became clear they were unconnected to this live investigation.</p> <p>Police queried the results with the TO who stated, contrary to their initial report, that the IP activity was system-driven. This meant the activity was unconnected to the authority's investigation.</p>
Consequence:	<p>An individual unconnected with the inquiry was questioned but no serious harm resulted.</p> <p>Under Section 231 (9) the IPC is only able to make a determination if the relevant error is made by a public authority. In this case no error by the public authority was made.</p>

Annex D: Communications Data

This annex details the use of communications data (CD) in 2019. The below tables give the number of applications made in relation to sensitive professions, the total number of applications submitted to OCDA, and a breakdown of applications from each agency.

Sensitive professions

In 2019, 50 law enforcement and public authorities applied for CD in relation to individuals of sensitive professions⁶⁹ (see also chapter 3).

Profession	
Lawyer	309
Journalist	116
Journalistic Source	15
Member of Parliament	138
Minister of Religion	135
Medical Doctor	300
Total	1,013

Applications submitted to OCDA

All non-urgent CD requests, other than those relating to journalists and those made by the UK's Intelligence Community (UKIC) are considered by the Office for Communications Data Authorisations (OCDA), who decides whether to approve the request. The below table breaks down the applications considered by OCDA from 26 April, when OCDA first accepted applications, up until 31 December 2019.

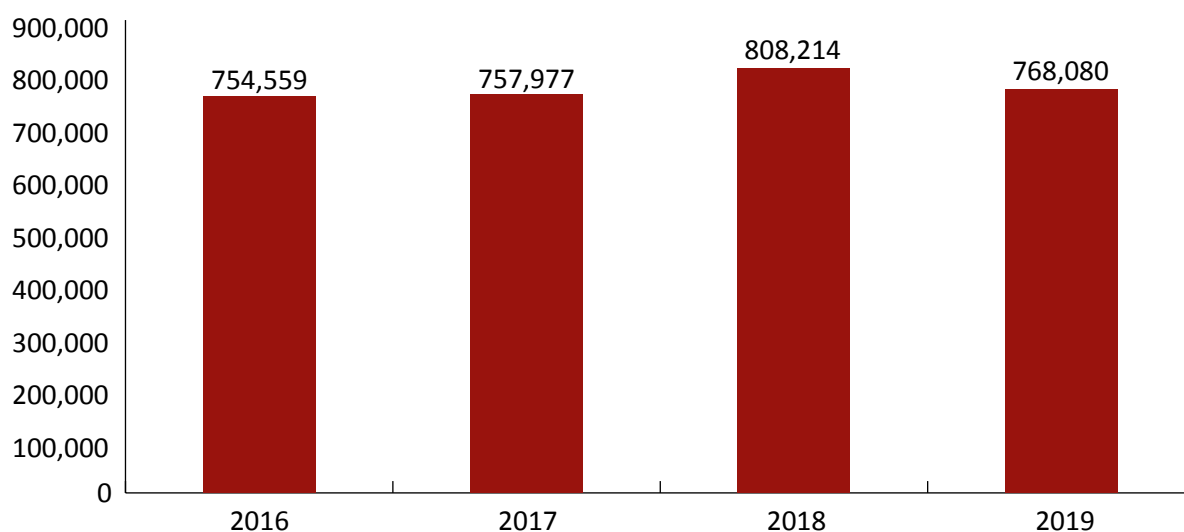
Total Applications received by OCDA	71,610
Decisions made	71,208
Authorised	63,688
Not authorised	7,520
Withdrawn	385
Applications with no decision (e.g. pending as at 31 December 2019)	17

⁶⁹ Note that this records all cases where the individual subject to the request is believed to hold a sensitive profession and does not reflect the intention to obtain sensitive material, or likelihood that sensitive material will be obtained.

Applications by public authority

As noted in previous chapters, the figures for the total number of CD items obtained is subject to a margin of error. We therefore cannot be confident whether fluctuations in these figures reflects a change in the number of items obtained. Nonetheless, changes in those figures have been proportionally minimal. In total, 768,080 items were obtained using targeted CD authorisations in 2019. This is broadly consistent with previous years as can be seen in the figure below.

Items obtained using targeted communications data authorisations 2016-2019



Name	Line Items	Type of Authority
Government Communications Head Quarters (GCHQ)	11,658	Intelligence Agency (UKIC)
MI5	20,176	Intelligence Agency (UKIC)
Secret Intelligence Service (SIS)	226	Intelligence Agency (UKIC)
Air Accidents Investigation Branch (AAIB) – Department for Transport (DfT)	5	Public Authority
Child Maintenance Group (Department for Work and Pensions)	0	Public Authority
Competition and Markets Authority	26	Public Authority
Criminal Cases Review Commission	3	Public Authority
Department for the Economy for Northern Ireland	4	Public Authority
Financial Conduct Authority	1,892	Public Authority
Gambling Commission	1	Public Authority
Gangmasters and Labour Abuse Authority	88	Public Authority
Health & Safety Executive	1	Public Authority
Health & Social Care Northern Ireland	0	Public Authority
Her Majesty's Prison and Probation Service	1,011	Public Authority
Independent Office for Police Conduct	91	Public Authority
Information Commissioner's Office	25	Public Authority
Maritime & Coastguard Agency	6	Public Authority
Maritime Accident Investigation Branch	1	Public Authority

Name	Line Items	Type of Authority
Medicines and Healthcare Products Regulatory Agency	163	Public Authority
National Anti-Fraud Network	1,379	Public Authority
Northern Ireland Prison Service	0	Public Authority
Office of Communications	10	Public Authority
Office of the Police Ombudsman for Northern Ireland	43	Public Authority
Police Investigations and Review Commissioner	1	Public Authority
Rail Accident Investigation Branch	16	Public Authority
Serious Fraud Office	423	Public Authority
Avon and Somerset Police	12,206	Police
Bedfordshire Police	7,680	Police
British Transport Police	3,481	Police
Cambridgeshire Constabulary	4,948	Police
Cheshire Constabulary	11,337	Police
City of London Police	3,586	Police
Cleveland Police	6,698	Police
Cumbria Constabulary	4,341	Police
Derbyshire Police	6,524	Police
Devon and Cornwall Police	17,296	Police
Dorset Police	4,234	Police
Durham Constabulary	5,792	Police
Dyfed Powys Police	3,953	Police
Gloucestershire Police	3,244	Police
Greater Manchester Police	41,394	Police
Gwent Police	6,689	Police
Hampshire Constabulary	8,512	Police
Hertfordshire Constabulary	13,903	Police
Her Majesty's Revenue & Customs (HMRC)	18,464	Law enforcement
Home Office Immigration Enforcement	7,146	Law enforcement
Humberside Police	9,780	Police
Kent and Essex Police	26,491	Police
Lancashire Constabulary	16,279	Police
Leicestershire Police	11,944	Police
Lincolnshire Police	4,076	Police
Merseyside Police	22,091	Police
Metropolitan Police Service Central Intelligence Unit (CIU)	116,171	Police
Metropolitan Police Service Department for Professional Standards (DPS)	2,220	Police
Metropolitan Police Service Counter Terrorism Command (SO15)	12,852	Police

Name	Line Items	Type of Authority
Ministry of Defence	105	Defence
Ministry of Defence (Intel) Intelligence	0	Defence
National Crime Agency	45,224	Law enforcement
Norfolk and Suffolk Constabulary	6,951	Police
North Wales Police	9,014	Police
North Yorkshire Police	5,433	Police
Northamptonshire Police	7,693	Police
Northumbria Police	9,624	Police
Nottinghamshire Police	10,593	Police
Police Scotland	50,959	Police
Police Service Northern Ireland	10,646	Police
Royal Air Force, Royal Military Police and Royal Navy Police	197	Police
South Wales Police	9,626	Police
South Yorkshire Police	9,075	Police
Staffordshire Police	8,680	Police
Surrey Police	5,066	Police
Sussex Police	7,609	Police
Thames Valley Police	14,057	Police
West Mercia and Warwickshire Police	22,329	Police
West Midlands Police	46,305	Police
West Yorkshire Police	28,194	Police
Wiltshire Police	5,476	Police

Annex E: Public Engagements

The Investigatory Powers Commissioner (IPC) undertook several public engagements in 2019. Details of those engagements are given below.

The CEO of the Investigatory Powers Commissioner's Office (IPCO) met oversight related Non-Governmental Organisations (NGOs) to discuss their interests in the use of investigatory powers and met representatives from Reprieve in September 2019.

Engagements with overseas bodies

Date	Event
4 February	meeting with Chair and General Secretary of the Commissie van Toezicht op de Inlichtingen – en Veiligheidsdiensten (CTIVD, or the "Review Committee on the Intelligence and Security Services:), The Netherlands (London)
7-8 March	European Oversight Bodies meeting (Brussels, Belgium). The IPC was represented by Judicial Commissioner Sir John Saunders and IPCO's CEO
6 to 9 May	visit by Margaret Stone, Inspector General of Intelligence and Security (IGIS), Australia (London)
31 July	meeting with Honourable Andrew Little, Justice Minister, New Zealand (London)
4 September	meeting with the Commission Nationale de Contrôle des Techniques de Renseignement (Paris, France)
8-9 October	UN International Intelligence Oversight Forum, London
15-17 October	Five Eyes Oversight Review Council (FIORC) meeting, London
11 November	meeting with the Independent National Security Legislation Monitor (INSLM) of Australia (London)
27 November	meeting with Chair and Deputy General Secretary of CTIVD, The Netherlands (London)
12-13 December	International Oversight Bodies Conference (The Hague, The Netherlands)

Meetings with Ministers

Date	Meeting
15 January	meeting with Rt Hon Ben Wallace MP, Security Minister, Home Office
1 April	telephone call with Rt Hon Ben Wallace MP, Security Minister, Home Office
16 April	meeting with Humza Yousaf MSP, Cabinet Secretary for Justice, Scottish Govt
7 October	meeting with Rt Hon Dominic Raab, Secretary of State for Foreign and Commonwealth Office

Engagement with NGOs and academics

Date	Event
19 June	meeting with Reprieve
3 December	meeting with the Kings College London Guardint project team

Engagement with the media

Date	Event
11 February	Interview with Joshua Rozenberg for Law Society Gazette ⁷⁰
20 May	interview with David Bond, for Financial Times ⁷¹

70 The Law Society Gazette, "Public trust in the post-Snowden secret state" (2 July 2018), <https://www.lawgazette.co.uk/commentary-and-opinion/public-trust-in-the-post-snowden-secret-state/5066698.article>

71 Financial Times, "New UK spying code rules out rendition of terror suspects" (24 May 2019), <https://www.ft.com/content/20c5df0e-7ca1-11e9-81d2-f785092ab560>

Investigatory Powers Commissioner's Office
PO Box 29105
London
SW1V 1ZU