

Annual Report of the Investigatory Powers Commissioner 2025

Annual Report of the Investigatory Powers Commissioner 2025

Presented to Parliament pursuant to section 234(6) of the Investigatory Powers Act 2016

Ordered by the House of Commons to be printed on 29 October 2026

Laid before the Scottish Parliament by the Scottish Ministers 29 October 2026

HC 253

SG/2026/138



© Crown copyright 2026

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.

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/official-documents.

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

978-1-5286-6754-8

E03653029 10/26

Printed on paper containing 40% recycled fibre content minimum

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

Contents

Letter to the Prime Minister	5
1. Introduction by the Investigatory Powers Commissioner, Sir Brian Leveson	6
2. IPCO: governance, resourcing and engagement	11
3. Regulatory and legislative matters	20
4. Oversight activities and challenges	32
5. Oversight activities and challenges: Agent X	47
6. Oversight activities and challenges: Northern Ireland	52
7. Errors and breaches	56
8. Litigation in 2025	69
9. Protecting confidential or privileged information	70
10. Technology	74
11. Technology Advisory Panel (TAP) Annual Report 2025	78
12. Statistics	81
Annex A. Definitions and glossary	104
Annex B. Budget	117
Annex C. Serious errors	119

Letter to the Prime Minister

The Rt Hon Sir Keir Starmer KCB KC MP
Prime Minister
10 Downing Street
London
SW1A 2AA

29 June 2026

Dear Prime Minister,

I enclose the Annual Report covering the work of the Investigatory Powers Commissioner's Office (IPCO) from 1 January to 31 December 2025.

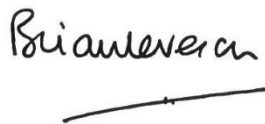
This report includes information on the use of covert powers by UK authorities, setting out the details required under section 234 of the Investigatory Powers Act 2016 (IPA). It is for you to determine, in consultation with my office, whether the report can be published in its full form without releasing 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 well-being of the UK or to the discharge of the functions of those authorities which I oversee.

As in previous years, I have written to you separately regarding certain sensitive details which I believe should not be published for reasons of national security.

The report identifies a number of issues and areas of concern arising from our oversight during 2025. Those matters are addressed in the report and, where necessary, in my separate correspondence.

They do not detract from the generally strong culture of compliance, dedication and professionalism shown across the authorities I oversee, but they do underline the importance of independent oversight and upholding safeguards.

Yours sincerely,

A handwritten signature in dark ink, reading "Brian Leveson". The signature is written in a cursive style with a long horizontal stroke at the end.

The Rt Hon Sir Brian Leveson
The Investigatory Powers Commissioner

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



*Sir Brian Leveson,
Investigatory Powers
Commissioner.*

I am pleased to present my Annual Report as Investigatory Powers Commissioner (IPC) for 2025. As set out in section 234 of the Investigatory Powers Act 2016 (IPA), I am required to report to the Prime Minister on how the Judicial Commissioners have carried out their functions during the reporting period.

In October 2025, I was appointed for a further term as IPC. This has given me the opportunity to reflect on what I have seen over the last six years. While my functions and my office (the Investigatory Powers Commissioner's Office – IPCO) have grown and evolved over this period, my purpose remains constant: to ensure that the State's use of covert investigatory powers, whether by the intelligence agencies, law enforcement or other public authorities, is carried out lawfully and in the public interest, that is to say when necessary, proportionate and with proper regard to rights to privacy.

Striking the right balance between protecting national security and preventing serious crime, on the one hand, and safeguarding individual rights, on the other, is never straightforward. The role performed by my office is therefore of real constitutional importance. In 2025, that importance was underscored by the scale of use of investigatory powers,¹ including the demand for prior authorisation where required and the increasing complexity of the technology through which the powers are exercised. Legal compliance and robust safeguards are not optional constraints: they are essential conditions for legitimacy and providing a "license to operate" for the intelligence agencies, law enforcement and other public authorities.

The importance of our oversight was also demonstrated by several disappointing instances that raised acute questions about compliance and candour. One such matter was the case of Agent X. In September 2025, I received a direction from the Prime Minister to investigate the circumstances in which false evidence was provided to the High Court and the Investigatory Powers Tribunal (IPT) in proceedings connected to that case. The Deputy Investigatory Powers Commissioner, Sir John Goldring, has led this work. The issues raised go to the heart of a system that, in part, depends upon the highest standards of candour from those subject to oversight. First, given the relatively small size of the Inspectorate at IPCO, we require candour from those whom we inspect to identify borderline or difficult cases all of which we will then examine: random selection can only go so far. Second, they also underline why independent, rigorous scrutiny is essential, not as an abstract safeguard, but as a practical mechanism for accountability that continues to learn and improve.

1 In 2025, 366,976 warrants and authorisations were issued across all public authorities.

Agent X was not the only significant issue in 2025. Across a number of public authorities, our inspections identified matters on which I have reported that require sustained senior attention. These are matters which I know have been taken seriously by the Heads of those organisations and are set out in detail in the chapters that follow. I highlight them here to signal the themes which run through the report: compliance, transparency and the need for public authorities to treat legal safeguards as integral to operational effectiveness.

First, the National Crime Agency (NCA) continued to report a higher number of errors than in previous years as well as backlogs in achieving compliant records and product management. Of particular concern were failings relating to the authorisation of a juvenile covert human intelligence source (CHIS) and the management of records relating to the use of CHIS and surveillance.

Second, in relation to His Majesty's Prison and Probation Service (HMPPS), my Inspectors identified recurring compliance concerns in the interception and monitoring of prisoners' communications. While I recognise the operational pressures within the prison estate, those pressures do not diminish the need for lawful, consistent and well understood arrangements. I have raised my concerns directly with HMPPS senior leadership, and IPCO will continue to monitor progress through inspection and engagement.

Third, in Northern Ireland, issues arose in relation to the identification and handling of cases that attract enhanced safeguards, including those involving confidential or otherwise sensitive material. The report of Angus McCullough KC into conduct by the Police Service of Northern Ireland (PSNI)² aligns with our findings on PSNI's performance, which provides welcome confirmation. However, it also provides evidence, insights and methods from which IPCO seeks to learn. At the same time, it is important to be clear about the nature of our role: we must provide effective assurance across a wide remit and a large number of public authorities, and we will continue to do so with rigour and independence.

Fourth, I remain concerned that the Government Communications Headquarters (GCHQ) has not yet established a sufficiently clear understanding of the scale, location and recoverability of lost removable media that may contain IPA-related data, notwithstanding that the underlying issues were first drawn to my attention several years ago. While I recognise the technical and practical challenges involved, the passage of time without a comprehensive account heightens the importance of sustained senior focus and assured remediation. Given the potential sensitivity of the material involved, I will continue to monitor progress closely.

Finally, in relation to the Ministry of Defence, my Inspectors identified shortcomings in its understanding and application of "The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees", with implications for the consistency and robustness of compliance. Actions have been issued to address these matters, and I will be keeping their implementation under close review to ensure that compliance improves and that the intended safeguards are fully embedded in practice.

Taken together, these matters also raise wider questions about whether parts of the investigatory powers framework, particularly in respect of older regimes such as the Regulation of Investigatory Powers Act 2000 (RIPA), remain clear, coherent and fit for purpose. Where we identify gaps, ambiguity or unintended consequences, I will continue to bring those issues to the attention of Government, and to engage constructively on any future legislative reform.

2 See: <https://www.mcculloughreview.org/>

The impact of technological change should not be underestimated. It brings major operational benefits to those charged with protecting the public, but it also increases the scale and complexity of intrusion that investigatory powers can enable, and it can have knock-on implications for the technology we all use on a daily basis living digitally enabled lives. This environment makes the work of Judicial Commissioners, the Technology Advisory Panel (TAP) and IPCO more demanding. While I am committed to meet those challenges, it is essential that I continue to keep our oversight methodology and the resources required to deliver it under review. The Spending Review settlement provides a measure of stability but demand continues to rise and the operational environment continues to evolve. I am therefore focused on modernising systems and processes, including exploring how automation and new technologies can support efficiency and sustainability, while ensuring that oversight judgments remain rigorous and independent.

These pressures have strengthened my resolve to be as transparent as possible about IPCO's work and about the use of investigatory powers, within the constraints necessary to protect national security and operational effectiveness. Transparency is vital to maintaining public trust and confidence in some of the most sensitive and powerful capabilities the State possesses. To that end, I have continued to speak publicly about IPCO's role. By demystifying what we do, and why we do it, we can support informed debate and strengthen confidence in independent oversight.

While this report highlights areas requiring improvement, I remain satisfied that independent oversight is working and that, among leaders of public authorities, there is a genuine commitment to compliance. Their challenge is to establish policies and systems that consistently deliver compliance and the candour on which our independent oversight relies. We cannot review all cases, so it is vital that public authorities highlight to us their problematic and complex cases, alongside our own selections.

Our increasing international engagement also provides reassurance that the UK's model continues to be regarded as a robust benchmark for independent scrutiny. In 2025, that engagement included bilateral discussions with international partners, a visit to Japan to discuss its cyber reforms and the hosting of the Five Eyes Intelligence Oversight and Review Council (FIORC) annual meeting in London. These relationships matter: they allow oversight bodies to compare approaches, share practical learning, and test our assumptions against the experience of peers operating in similarly complex environments.

The use of investigatory powers remains high, and this report sets out the scale of IPCO's authorisations and oversight work undertaken during 2025. It also records where errors occurred and how those matters were addressed. Across the breadth of the system, public authorities take their legal obligations seriously and engage constructively with IPCO. Where we identify non-compliance, our role is to ensure it is recognised, remedied and learned from, so that safeguards operate effectively in practice, not only in principle.

Finally, I am conscious that public confidence in investigatory powers rests on a simple proposition: that powers will be authorised, used proportionally and only when necessary, and that they will be subject to meaningful independent scrutiny. In 2025, IPCO has continued to provide that scrutiny, consistently and rigorously and, where possible, transparently.

Key issues covered in this report



This table highlights the principal issues examined in this report, providing a quick reference to the relevant sections.

1	Implementation of Parts 7A and 7B of the IPA Following the new requirements brought in under the Investigatory Powers (Amendment) Act 2024 (IP(A)A), we have considered applications in relation to bulk personal datasets (BPD) where there is a low or no reasonable expectation of privacy and use of third party personal datasets. [See: paragraphs 3.2 - 3.9]
2	Access to records and inspection methodology We have changed how we select and access MI5 covert human intelligence source (CHIS) records, learning from our 2022 Agent X inspection report and piloting a new approach in 2025. [See: paragraphs 4.12–4.14].
3	Ministry of Defence (MoD) We set out concerns around the MoD's application of "The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees" [see: paragraphs 4.79-4.80] as well as issues about its risk assessments relating to CHIS, including an error relating to the welfare and security of one of its CHIS. [See: paragraphs 4.15-4.18].
4	Safeguarding and records management We continue to be concerned about work by the Government Communications Headquarters (GCHQ) to account for removable media potentially containing IPA-related data. [See: paragraphs 4.66-4.68]
5	International data sharing During our 2025 inspection, we found that GCHQ had appropriate safeguards of confidential information resulting from bulk interception for its own analysts but we raised significant concerns about whether overseas partners were complying with enhanced protections for journalistic and legally privileged material. [See: paragraphs 4.35-4.38]
6	Interception by His Majesty's Prison and Probation Service (HMPPS) Inspections of interception and monitoring practices across the HMPPS prison estate revealed recurring compliance issues with the Prison Rules and the Authorised Communications Controls and Interception Policy Framework (ACCIPF). [See: paragraphs 4.41-4.44].
7	National Crime Agency (NCA) operational records During our 2025 CHIS and surveillance inspection of the NCA, we identified a compliance issue in relation to its management of operational records, with the NCA unable to demonstrate consistently that CHIS, undercover and other RIPA-related material was being reviewed, retained or disposed of in accordance with legislative requirements and relevant Codes of Practice. [See: paragraphs 4.64-4.65]
8	Agent X Chapter 5 sets out our involvement on the matter before 2025, the Divisional Court and Investigatory Powers Tribunal (IPT) judgments in July 2025 and our work on the investigation that we were directed to undertake by the Prime Minister. [See: chapter 5].
9	Northern Ireland This chapter summarises the oversight issues that arose in Northern Ireland during 2025. It draws together the IPT litigation, the independent Angus McCullough KC review of Police Service of Northern Ireland (PSNI) practice and the steps we have taken to strengthen how cases involving how confidential material are identified, recorded and brought to our attention. [See: chapter 6].

Key issues covered in this report

10

Errors

In 2025, there was an increase in the number of errors by the UK intelligence community (UKIC) and the NCA. [See: chapter 7]. In addition, the Investigatory Powers Commissioner (IPC) found that four errors met the serious error definition.

2. IPCO: governance, resourcing and engagement

Overview

- 2.1 This chapter summarises key developments within the Investigatory Powers Commissioner's Office (IPCO) in 2025. It sets out how we planned for the Spending Review, worked on the Home Office's review of the IPCO funding model and how we managed recruitment constraints. It also covers the work we did to improve operational resilience through targeted investment in internal systems, including our warrant processes and the Case Management System (CMS) used for communications data (CD) authorisations. Finally, the chapter describes how we supported our staff through internal communications and learning and development (L&D), and how we strengthened our external communications and engagement with public authorities, civil society, the media and international partners.

Resourcing and financial planning

- 2.2 The Investigatory Powers Act 2016 (IPA) sets out the following in section 238(2) in regard to the duty of the Secretary of State to provide the Investigatory Powers Commissioner (IPC) with the staff, accommodation, equipment and other facilities necessary to carry out the IPC's functions:

The Secretary of State must, after consultation with the Investigatory Powers Commissioner and subject to the approval of the Treasury as to numbers of staff, provide the Judicial Commissioners with—

- (a) such staff, and*
- (b) such accommodation, equipment and other facilities and services, as the Secretary of State considers necessary for the carrying out of the Commissioners' functions.*

Spending Review 2025

- 2.3 Since 2024, we have worked closely with the Home Office as part of its Spending Review preparations to ensure that we continue to receive the resources we need to fulfil the IPC's statutory responsibilities.
- 2.4 We are content with our Spending Review settlement for 2026/27–2028/29. In the first year the Home Secretary has allocated £16.6 million to the IPC to support the delivery of his statutory functions through IPCO. We will update on future financial allocations in future Annual Reports.

- 2.5 Although this does not allow us to grow our operations to meet rising demand, the settlement represents a better outcome than was anticipated during parts of the planning phase. For context, applications for CD have increased by an average of 9% year-on-year, including during the period from 2024 to 2025. The multi-year settlement also provides the certainty needed for long-term financial and business planning.
- 2.6 We have developed a three-year budget that prioritises frontline delivery of our authorisation and oversight capabilities as well as identifying and reinvesting efficiencies. This will enable the IPC to oversee and authorise the use of investigatory powers while remaining within the funding envelope set by the Home Secretary.
- 2.7 In 2025, we operated under a recruitment freeze, limiting our ability to replace leavers or create new posts. We prioritised critical posts and redistributed work to maintain authorisation and oversight functions while remaining within Home Office controls.
- 2.8 During the year, once we were confident that the Spending Review would provide financial stability for the coming years, we also continued to modernise our internal systems. This included investment in improvements to our warrant processes and enhancements to the CMS, which plays a central role in handling CD applications. These upgrades formed part of a wider programme to strengthen system resilience and support more efficient and sustainable authorisations processes. Further details are set out in the Technology chapter of this report.³

Funding model

- 2.9 In 2025, we provided information in response to a request from the Home Office to review the IPCO funding model. As highlighted at paragraph 2.2, there is a duty on the Home Secretary to provide the necessary resources to the IPC to enable the Commissioner to fulfil their statutory duties. It is up to the Home Secretary, supported by their officials, not only to determine the amount of funding, but also how it is to be provided. Whether and when to alter the current funding model is a decision for the Home Office.

Internal communications and staff engagement

- 2.10 Keeping our people informed and connected remained central to how we operated. In 2025, we continued to develop our internal communications to support openness and ensure staff across all locations felt informed and engaged.
- 2.11 Our monthly internal bulletin remained a key channel for sharing news, updates and achievements across the organisation. Quarterly all-staff calls provided opportunities for colleagues to hear directly from senior leaders on strategic priorities, ask questions and contribute to discussion.
- 2.12 Twice in the year, we brought colleagues together in person for our IPCO staff-days held in our offices in Manchester, Birmingham and London. These events reflected our commitment to learning, collaboration and building a positive organisational culture. The days reflected our commitment to learning, collaboration and building a strong organisational culture.
- 2.13 We continued to strengthen two-way dialogue and ensure staff had opportunities to share ideas and feedback.

3 See: chapter 10.

Learning and development

- 2.14 We continued to build our L&D offer throughout 2025, adding core skills resources, lunch and learn sessions and a quarterly newsletter. New induction materials were rolled out for all new joiners to IPCO, alongside a tailored programme for incoming Judicial Commissioners with support from the Legal Team and Inspectorate.
- 2.15 Operational staff were expected to remain up to date on emerging techniques and legislation, supported by a varied approach to CD legal issues (Judicial Commissioner input, fact sheets, and practice-development sessions). This training will continue in 2026, with specialist topics led by the Legal Team.

External communications and stakeholder engagement

- 2.16 In 2025, we published a summary of our revised external communications and engagement strategy,⁴ setting out how we will use communications and stakeholder engagement to support our mission of protecting human rights through independent oversight. The strategy focused on strengthening public understanding of investigatory powers, building confidence in our independence and demonstrating active engagement with a diverse range of stakeholders.
- 2.17 Building on the foundations laid in 2024, we significantly expanded our digital presence and content output. We launched a YouTube channel and a LinkedIn page, complementing our existing presence on X,⁵ to share video content directly with stakeholders, including regular updates from the IPC on our work and activities. These new channels helped us reach wider and more varied audiences and build a strong and growing following. We also invested in our communications infrastructure, procuring mailshot functionality to enhance how we distribute content to stakeholders.
- 2.18 We continued to engage proactively with the media throughout 2025. The Technology Advisory Panel's (TAP) publication of its "Artificial Intelligence (AI) Proportionality Assessment Aid" generated significant interest, leading to media interviews and coverage in trade press.⁶ The IPC also contributed to opinion pieces, helping to shape public discourse on oversight and investigatory powers.
- 2.19 The IPC delivered the annual Atkin Lecture at the Reform Club and spoke to national security students at King's College London. He also chaired a panel discussion for the Centre for Emerging Technology and Security (CETaS) and made his first appearance on Joshua Rozenberg's "A Lawyer Talks" podcast.⁷ These engagements provided valuable opportunities to discuss oversight, technology, and the balance between privacy and security with a wide range of audiences.
- 2.20 Throughout the year, we showcased the IPC's interactions with the Government, Parliament and the international oversight community through our social media channels, reinforcing our commitment to transparency about the work we do.

4 See: IPCOs-External-Communications-and-Engagement-Strategy-2025.pdf

5 See: LinkedIn | X @IPCOoffice and IPCO – YouTube

6 See: AI-Assessment-Framework.pdf

7 See: Watching the watchers – by Joshua Rozenberg

Engagement with non-governmental organisations (NGO)

- 2.21 In 2025, the IPC continued to prioritise open and constructive dialogue with civil society organisations, recognising their important role in contributing to public debate on investigatory powers and oversight.
- 2.22 Throughout the year, the Chief Executive met with representatives from key organisations, including Big Brother Watch and Amnesty International, to discuss areas of shared interest and hear external perspectives on our work.
- 2.23 The IPC also hosted a NGO roundtable, which provided an opportunity for civil society representatives to discuss the findings of our 2024 Annual Report, an event which we plan to run annually. This year's session brought together representatives from Big Brother Watch, the Open Rights Group, Privacy International and Reprieve. Topics discussed included error reporting and transparency, the oversight of AI and emerging technologies, thematic warrants and end-to-end encryption.
- 2.24 These conversations continued to inform our work and helped build public confidence in the investigatory powers oversight regime.
- 2.25 The following graphic illustrates the engagements undertaken by the IPC in 2025. In addition to the listed meetings, the IPC regularly meets with authorities under his oversight.

Public engagements

13 February – Interview with Joshua Rozenberg	13 February – Speech to Reform Club
10 March – Speech to International Symposium on Lawful Access	19 March – The Rt Hon Lord Hermer KC, Attorney General
27 March – Speech to King's College London	2 April – The Rt Hon Dan Jarvis MP, Security Minister, Home Office
8 April – The Rt Hon Yvette Cooper MP, Home Secretary	13 April – Chief Constable Trevor Rodenhurst, NPCC lead for ROCUs and Undercover Policing
15 April – Chief Constable Jo Farrell QPM, Police Scotland	15 April – Angela Constance MSP, Cabinet Secretary for Justice and Home Affairs, Scottish Government
29 April – Panel chair at CETaS event, Turing Institute	19 May – Speech for GCHQ National Security Law and Policy series
4 June – The Rt Hon Lord Beamish (Chair) and the Rt Hon Sir Jeremy Wright KC MP (Deputy Chair), Intelligence and Security Committee	10 June – The Rt Hon Yvette Cooper MP, Home Secretary
1 July – Speech to International Communications Data and Digital Forensics Conference	16 July – IPCO-hosted NGO roundtable event
14 July – The Rt Hon Lord Justice Singh, Investigatory Powers Tribunal	31 July – John Edwards, Information Commissioner
27 August – John Wadham, Human Rights Advisor, Northern Ireland Policing Board	10 September – Chief Constable Jon Boutcher QPM, Police Service of Northern Ireland (PSNI)
27 October – The Rt Hon Shabana Mahmood MP, Home Secretary	3 November – Speech to Homeland Security Group, Home Office
9 December – Roundtable event at Global Centre for Democratic Constitutionalism	18 December – Lady Carmichael (President) and Lord Boyd (Deputy President), Investigatory Powers Tribunal
18 December – Chief Constable Jon Boutcher QPM, Police Service of Northern Ireland (PSNI)	

International engagement and strategy

- 2.26 In 2025, we strengthened our international partnerships and engagement, reflecting both the growing international interest in the UK's oversight model and the increasingly global nature of intelligence oversight challenges. Activities spanned multilateral forums, bilateral cooperation and specialist networks, enabling us to share expertise, learn from comparator bodies and contribute to shared understanding of complex oversight issues. These engagements supported our work by enhancing insight, fostering innovation and deepening relationships with organisations facing similar demands in an evolving technological and geopolitical landscape.

Five Eyes Intelligence Oversight and Review Council (FIORC) conference

- 2.27 In October 2025, we hosted the 2025 annual meeting of the Five Eyes Intelligence Oversight and Review Council (FIORC).

What is FIORC?

FIORC brings together the independent intelligence oversight and review bodies from the Five Eyes countries. Its members are:

- **Australia:** Office of the Inspector General of Intelligence and Security-General of Intelligence and Security
- **Canada:** Office of the Intelligence Commissioner; and National Security and Intelligence Review Agency
- **New Zealand:** Commissioner of Intelligence Warrants; and Office of the Inspector General of Intelligence and Security-General of Intelligence and Security
- **United Kingdom:** IPCO
- **United States:** Office of the Inspector General of the Intelligence Community

The Council enables members to exchange views on issues of shared interest, compare oversight methodologies and explore areas where cooperation is appropriate. FIORC also promotes transparency, where possible, to support public confidence, and maintains contact with political offices, oversight committees and relevant partners, including non-Five Eyes countries.

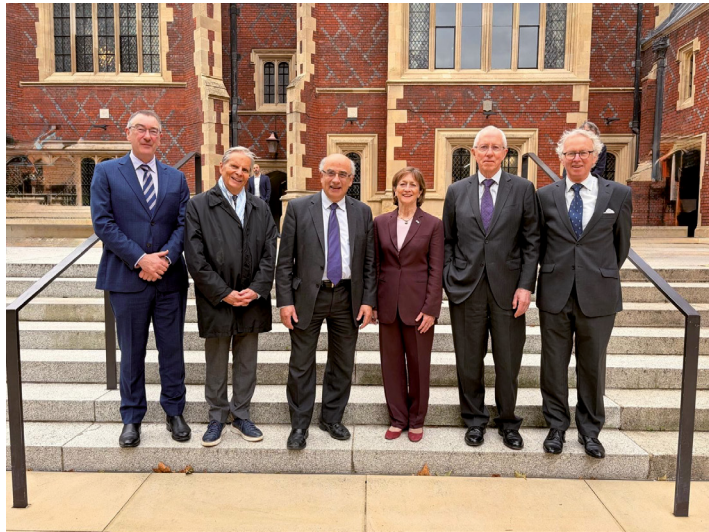
FIORC operates under a Charter (see 2.31-2.32).⁸

- 2.28 The meeting provided an opportunity to strengthen cooperation across the Council and to consider shared challenges in the oversight of intelligence and security activity. Discussions focused on transparency, emerging technologies, AI, legal developments and longer-term strategic priorities. Members acknowledged the increasingly complex operational environment and reaffirmed the importance of strong, independent oversight in maintaining public trust.

8 See: FIORC Charter – 2025

2.29 Other key areas covered were:

- the importance of strong, open relationships between oversight bodies and regulated agencies, supported by operational understanding and timely access to information;
- different approaches to how oversight bodies respond to significant non-compliance, noting that transparency, proportionality and clarity of purpose underpin effective remedial action, including where exceptional interventions are required;
- the importance of transparency to maintaining public confidence, with members discussing approaches to public reporting, parliamentary engagement and engagement with civil society within lawful constraints;
- the impact of technological change on intelligence activity and the need for oversight to keep pace, including updates on approaches to oversight of AI; and
- different approaches to oversight of technological vulnerabilities and the need to balance national security, cybersecurity and the public interest.



FIORC Principals at Lincoln's Inn.

2.30 A key outcome of the meeting was the agreement of updates to the FIORC Charter. Developed through the Council's legal network, the revised Charter enhances governance arrangements and introduces a rotating secretariat to support shared leadership.

2.31 The Council agreed several priorities for the year ahead, including continued development of the thematic networks established in 2024, strengthened collaboration on transparency, AI oversight and open-source intelligence, and implementation of the revised FIORC Charter.



FIORC Principals signing the revised FIORC charter.

2.32 Further details are available in the Executive Summary.⁹

⁹ See: 2025_Annual_FIORC_Meeting_Executive_Summary_Final.pdf

Other international engagements

- 2.33 In addition to FIORC, we also engaged extensively with international partners throughout 2025. These engagements strengthened relationships with peer oversight bodies, supported the exchange of practical learning and contributed to wider international discussions on technology, data governance and evolving oversight approaches.



Overview of IPCO's international engagements and bilateral meetings held during 2025.

- 2.34 During the year, we participated in several European and multilateral forums, including the European Intelligence Oversight Network (EION), where discussions focused on the acquisition and use of commercially available sensitive data by national security agencies. We also took part in the European Intelligence Oversight Conference (EIOC) in November, contributing to sessions on access controls, data quality, institutional independence and the operational impact of technological change. Alongside these engagements, we continued regular exchanges with longstanding European partners through conference participation, knowledge-sharing events and ongoing discussions on oversight methodology, transparency practices and inspection processes.
- 2.35 We continue to be an active member of the Intelligence Oversight Working Group (IOWG). We attended the technical and staff meetings in Copenhagen in May and the chairs, technical and staff meetings in Zurich in November. These meetings provided opportunities to share insight on inspections, technology, and oversight in increasingly complex operational environments. Work also began to prepare for the IOWG meeting in October 2026, which we will host in the UK.



IOWG Chairs in Zurich.

2.36 In January 2025, the IPC was invited to Japan to discuss the UK oversight model with Ministers and senior officials, followed in June by further engagements with Minister Taira, Japan's Minister for Cybersecurity, and Hiroshi Suzuki, Ambassador of Japan to the UK. We also hosted a follow-up visit from a Japanese legal delegation to discuss inspection methodology, transparency practices and the use of technology in oversight.



The Investigatory Powers Commissioner, Sir Brian Leveson (left), with Itsunori Onodera MP, Chairman of Japan's Policy Research Council (right), January 2025.

2.37 In May 2025, IPCO officials were invited to speak at the UN Security Council Counter-Terrorism Executive Directorate (CTED) conference in Jakarta, focusing on strengthening oversight and accountability across South and South-East Asia. We presented on independent authorisation of investigatory powers, the double lock, and our approach to assessing necessity and proportionality. We also participated on a panel on oversight in the digital age and presented on the workings of the TAP, in relation to oversight of public authorities' use of AI. In November, we were invited to join a panel discussion at the International Intelligence Oversight Forum (IIOF) in Texas, contributing to wider dialogue on global oversight challenges.

2.38 Our international engagement during 2025 demonstrated both the increasing expectations placed on oversight bodies and growing interest in our approach. We will continue to keep our approach to international engagement, and the strategy which underpins it, under review to ensure effectiveness and value for money.

3. Regulatory and legislative matters

Overview

- 3.1 This chapter sets out the main regulatory, policy and legal developments that affected the work of the Investigatory Powers Commissioner (IPC), the Judicial Commissioners and the Investigatory Powers Commissioner's Office (IPCO) during 2025. It covers the continued implementation of the Investigatory Powers (Amendment) Act 2024 (IP(A)A), including the commencement of the warrant requirement for examining third party bulk personal datasets (BPDs) and the inspection work that followed. It also summarises our conclusions on thematic warrants, which we issued to improve consistency and legal certainty in applications. The chapter then describes some other matters that arose during the year, including issues relating to Home Office Handling Arrangements, our statutory functions under Schedule 3 to the Counter-Terrorism and Border Security Act 2019, support to public inquiries, disclosures made to IPCO under the information gateway, and work to protect IPCO's independence where public authorities sought to impose additional vetting checks on Inspectors.

Implementation of the Investigatory Powers (Amendment) Act 2024

Bulk personal datasets: low or no reasonable expectation of privacy

- 3.2 In 2025, the intelligence agencies applied for a number of category authorisations under Part 7A of the Investigatory Powers Act 2016 (IPA). Under section 226BB(1)(b), a Judicial Commissioner must review, applying judicial review principles, "whether section 226A applies to any dataset that falls within the category of datasets described in the application". The IPC considers that section 226BB requires the Judicial Commissioner to be able to make a judgment from the category's description as to whether, on the balance of probabilities, only low/no datasets would be likely to fall within the category. It was difficult to see how Parliament could have intended any reading that would leave room in a category for any dataset that was not likely to be 'low/no'. When scrutinising a category authorisation, there are two principal issues: whether it is possible to identify, with sufficient clarity and precision, the scope of the category of datasets for each authorisation; and whether the nature of any dataset falling within the category is such that the individuals to whom the personal data relates could have no, or only a low, reasonable expectation of privacy (REOP) in relation to the data.
- 3.3 The IPA sets out non-exhaustive factors which must be taken into account when considering a data subject's REOP in a dataset. Those factors are:
- the nature of the data;
 - the extent to which-
 - the data has been made public by individuals, or
 - the individuals have consented to the data being made public;

- if the data has been published, the extent to which it was published subject to editorial control or by a person acting in accordance with professional standards;
 - if the data has been published or is otherwise in the public domain, the extent to which the data is widely known about; and
 - the extent to which the data has already been used in the public domain.¹⁰
- 3.4 The IPC provided substantial feedback on the initial category authorisation applications from the Secret Intelligence Service (SIS), in line with the engagement between public authorities and Judicial Commissioners enabled under section 232(2) of the IPA. He identified that SIS's descriptions of categories lacked sufficient clarity and were of a breadth that made it difficult to conclude that the datasets that would be covered would be limited to low/no REOP. The IPC observed that, just because data might be in the public domain, it did not necessarily render the data low/no REOP. It was important for applicants to consider the extent to which the dataset had been proliferated in the public domain and over what duration. A data subject's REOP is likely to diminish the more widely their data has been publicly disseminated and as time passes. This is especially the case in respect of any 'hacked' or leaked datasets. SIS ultimately withdrew all these initial applications for category authorisations following feedback conveyed as part of requests for further information. This is a paradigm example of us exercising effective *ex ante* oversight which is not reflected in our statistics for the number of applications refused.
- 3.5 By the end of 2025, both SIS and the Government Communications Headquarters (GCHQ) had successfully obtained category authorisations.
- 3.6 During our 2025 inspections, we did not identify any concerns with the UK intelligence community's (UKIC) assessment of low/no REOP in respect of datasets obtained under internally authorised "individual authorisations" under the categories approved by a Judicial Commissioner. However, we identified that GCHQ had erroneously authorised the retention of multiple datasets under an individual authorisation. The datasets in question all had an identical necessity and proportionality case and the IPC acknowledged that GCHQ's rationale in grouping them together was understandable, but nonetheless incorrect. The IPC held that an individual authorisation can authorise the retention of only a single, individual, dataset.
- 3.7 As requested by the Security Minister in 2024, we will continue to keep Part 7A authorisations under careful scrutiny until we are satisfied completely with the procedures in place.

Third party bulk personal datasets

- 3.8 On 25 April 2025, the requirement for an authorisation by warrant to examine a third party BPD came into force.¹¹ This followed the commencement of the power for the intelligence services to obtain such a warrant from 14 October 2024. As well as authorising new accesses, applications also covered existing accesses that were of critical importance to maintain for national security. The commencement of the requirement necessitated collaboration between warrant requesting agencies and warrant granting departments (WGDs) before new applications could be considered by Judicial Commissioners. In the event, commencement occurred with applications from some agencies not being approved. It was recognised by the agencies and departments involved that the implementation was

¹⁰ Section 226A(3) of the IPA

¹¹ Section 226F of the IPA

not as smooth as it should have been. This resulted in an HMG-led lessons learnt exercise, to which we contributed, and which identified a number of improvements for processes and ways of working relating to the implementation of new powers.

- 3.9 The focus of our BPD inspections during 2025 was on post implementation activity including the establishment of governance structures that enable each agency to assess, warrant and review datasets. We also focussed on reviewing access control mechanisms and audit, how sensitive personal data is further protected and the provision of staff training.

Thematic warrants

- 3.10 In 2023, we conducted a review of thematic warrants following concerns regarding inconsistencies in applications arising from different interpretations of thematic warrant categories described in the IPA. As set out in our 2024 Annual Report, we shared and discussed our findings with the Home Office and the operational community. In 2025, following that consultation, we circulated the conclusions from our findings to the relevant public authorities setting out the IPC's legal position on the use of the different statutory thematic warrant categories/types. These conclusions largely consolidated views already expressed by Judicial Commissioners through the consideration of applications. Judicial Commissioners began considering the conclusions from our findings in relation to applications for new warrants and renewals from January 2026.
- 3.11 We consider that setting out these findings will improve the drafting of thematic warrants and promote greater consistency of approach from both applicants and decision makers. A summary of some of our findings are set out below.

Summary of IPCO findings

Definition and statutory basis

The subject matter categories are defined in sections 17 and 101 of the IPA and an explanation of what is required in the warrant is further set out in sections 31 and 115 of the IPA. Any subject matter category that is chosen must be necessary and proportionate in the circumstances.

Legal certainty and foreseeability

This is a critical principle. Warrant parameters must be clear and foreseeable to avoid becoming an unlawful general warrant. It must always be possible to know who or what is covered, and who or what is not. If the description of an activity, purpose, group, or investigation lacks legal certainty, the warrant will not be approved by a Judicial Commissioner.

Using subject matter general descriptors

A thematic warrant can include multiple subject matter general descriptors, but only if all persons fall within a single investigation or operation, or a single overarching common purpose or particular activity. Descriptors provide greater particularisation of a group, but the group must be under one theme (e.g., one investigation).

Justifying a thematic warrant

Applications must explain why a thematic warrant is appropriate and proportionate. It must also explain why individual warrants are not practicable or desirable. There must also be a justification for any general descriptor: why it is not reasonably practicable to name individuals. A thematic warrant with a broad targeting discretion may be disproportionate if individual or separate warrants would achieve the same result.

Urgency and operational agility

If urgency or agility is relied upon to justify the breadth of a warrant, the applicant must explain why urgent non-thematic warrants or modifications would not be more appropriate or proportionate. Different standards apply to urgency and operational agility. Operating at scale (e.g., widespread threat) may justify a thematic approach, but will be subject to close scrutiny by IPCO.

Naming persons of sustained intelligence interest

There is no legislative obligation to add individually by name a person who falls within a general descriptor and is subsequently identified. However, where proportionality is finely balanced, the Judicial Commissioner may expect the public authority to undertake to add individuals by modification once they become of sustained intelligence interest. Applications should explain how a public authority will manage persons of sustained intelligence interest.

Groups

A "group" is defined only by the common purpose or particular activity. No further connection (e.g., by location or time) is required. Multiple sub-groups (e.g., different terrorist organisations with the same ideology) can be included if they share the same theme.

Particular activities vs. other categories

"Particular activity" has an ordinary meaning but must be articulated with sufficient specificity to understand it. Multiple related verbs (e.g., preparing, planning, conducting acts of Islamist terrorism) may form one particular activity. However, overly broad themes (e.g., preparing any type of terrorism) may, depending on the context, lack sufficient particularity. The distinction with "activities of a particular description" (for equipment interference only) does not narrow the interpretation of "particular activity".

Common purpose

"Common purpose" should be used cautiously: groups with similar ideologies may not necessarily share a common purpose. Principles from criminal law concerning "conspiracy" are helpful, but not determinative.

Single investigation or operation

Single investigation or operation must be given its ordinary meaning. Applications must be explicit in explaining why the activity is one single investigation or operation and address any counterpoints.

Distinction from bulk warrants

Only intelligence services may obtain bulk warrants, but where targeted warrants are broad in scope it may result in obtaining a large amount of data. Applicants must consider whether the conduct is more appropriately authorised under a bulk warrant. A targeted thematic warrant may still involve very large numbers of targets (e.g., thousands of EncroChat users) with the possibility of collateral intrusion. However, this can be contrasted with bulk warrants which will intentionally cover a very large number of persons who are not of intelligence interest.

Legal advice

It is important for applicants to seek legal advice in novel or complex cases. IPCO will not act as a legal adviser and will not lower standards for public authorities who fail to consult their lawyers.

Operational purposes

- 3.12 Over the past few years, and as mentioned in our last Annual Report, we have been reviewing the specificity of operational purposes. Operational purposes are a means of categorising the purpose for which a bulk warrant is authorised. Our review stemmed from the judgment of the Grand Chamber of the European Court of Human Rights (ECHR) in *Big Brother Watch* and the Court of Appeal in *Liberty v SSHD*.¹² The European Court of Human Rights held that a bulk interception warrant should “at the very least identify the categories of selectors to be used”. In the context of warrants for bulk communications data (CD), the Court of Appeal in *Liberty* held that:

“the need to specify the operational purposes, and the need for the Secretary of State, and the Judicial Commissioner to consider each specified operational purpose is necessary and that the examination of communications data is necessary for those specified operational purposes will act as a constraint upon the examination of such material and does ensure an adequate degree of control over the range of CD that may be selected for examination.”

- 3.13 The Court of Appeal therefore concluded that operational purposes were a meaningful restriction and we see no basis to distinguish the Court’s reasoning here in the context of bulk CD from bulk interception. It follows that the oversight purpose of requiring approval of the categorisation of selectors can be achieved by the specification of operational purposes, provided, of course, that the operational purposes are sufficiently specific to constitute a “meaningful restriction”.
- 3.14 Although all bulk warrants specify operational purposes chosen from a central list maintained by the heads of the intelligence services, our focus has been on bulk interception given the context of *Big Brother Watch*. At our request, the Home Office undertook a review of the specificity of operational purposes in 2023. We concluded from this review that, before reaching any conclusion as to specificity of the operational purposes, it was necessary to first explore with GCHQ whether it would be technically and operationally feasible to modify an operational purpose. GCHQ has confirmed that it is able to modify them and accepts that an operational purpose need not be on the bulk

12 *Big Brother Watch v United Kingdom* [2021] ECHR 58170/13 (paragraph 354). See: BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM and *Liberty v SSHD* [2023] EWCA Civ 926 (paragraph 138). See: National Council for Civil Liberties, R (On the Application Of) v Secretary of State for the Home Department & Anor [2023] EWCA Civ 926 (04 August 2023)

interception warrant at the point the warrant is issued in order to select communications for examination that have been intercepted under that warrant. It is sufficient for a corresponding operational purpose to be added subsequently by way of warrant modification; this would enable the examination of content intercepted prior to the modification.¹³

- 3.15 The IPC considered the Home Office's submission that a bulk interception warrant can be issued with an operational purpose that "may be" or "is" necessary, which differed from our analysis. Section 138(1)(d) of the IPA sets out the relevant test for a bulk interception warrant. It states that:

"The Secretary of State may, on application made by or on behalf of the head of an intelligence service, issue a bulk interception warrant if-

...

(d) the Secretary of State considers that-

(i) each of the specified operational purposes (see section 142) is a purpose for which the examination of intercepted content or secondary data obtained under the warrant is or may be necessary, and

(ii) the examination of intercepted content or secondary data for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary."

- 3.16 This is a two-stage test. First the Secretary of State must consider that each operational purpose on the warrant is one on the central list and is a purpose for which examination is currently necessary or may be necessary in the future. (This is simply incorporating the test that the Secretary of State has already had to apply in order to approve the addition of the operational purpose to the central list). It ensures that this test is reviewed personally by the Secretary of State who actually decides to issue the bulk warrant in question (which may of course not be the same person).
- 3.17 The second stage (limb (ii)) requires the Secretary of State to be satisfied that examination is currently necessary (at the point the warrant is issued) on national security grounds. There is no "may" in the second limb. This makes logical sense because even a bulk warrant must be proportionate and Parliament has provided a mechanism for modification of the operational purposes. Even if the Home Office's analysis was correct on this point, it would weaken the argument that the operational purposes, as a categorisation of selectors, provide a meaningful restriction.
- 3.18 With the understanding agreed with GCHQ that it is feasible to modify an operational purpose, we revisited the Home Office's conclusions of its 2023 review. Although a modification to a bulk interception warrant's operational purpose might not be immediate, GCHQ would not be in a materially different position from any interception authority needing to make an urgent modification to a targeted warrant, were the interception for a purpose not covered under a current operational purpose; this is consistent with the urgency procedure provided for by Parliament.

13 Operational purposes govern the selection for examination of communications by analysts and not the automated interception of unselected communications.

- 3.19 Save for some minor queries, the IPC confirmed in December 2025 that he was content with the specificity of all but one of the operational purposes. The IPC advised that the purpose in question should be broken up as it covered matters that were conceptually distinct, and because doing so would provide the Secretary of State with more choice when deciding whether “the examination of intercepted content or secondary data for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary” (see section 138(1)(d)(ii) of the IPA).
- 3.20 The IPC did not propose a reduction in the matters on the central list of operational purposes and suggested that the central list may merit some expansion to accommodate greater specificity. The IPC was content that the central list should include every conceivable current and future operational purpose and provide a full “à la carte” menu for the heads of the intelligence services to choose from when applying for a bulk warrant. However, each intelligence service may not have a need for all operational purposes all the time, reflecting their differing functions and operational priorities. It is important to emphasise that no privacy intrusion arises from the central list alone, what matters is what operational purposes are listed on the bulk warrant itself. Operational purposes which do not correspond to current operational requirements should not be included on bulk warrants.
- 3.21 The IPC accepted that the vast majority of operational purposes should be on each bulk interception warrant. However, he concluded that warrants can, and should, be modified (on an urgent basis if necessary) to add an operational purpose from the central list. The combined expertise of the three agency heads in producing the central list should be effective mitigation of intelligence failure from omitting something from that list, and the IPC noted that the central list has not needed modification to date.
- 3.22 The Home Office will need some time to review with UKIC the IPC’s comments on the 2023 Review and engage with us as necessary in order to endeavour to reach agreement on a final list. It is expected that the Home Office will conduct this expeditiously and, once any update to the central list has been formally completed, the intelligence services will wish to review their bulk warrants and modify accordingly.

Annual Review

- 3.23 The IPA requires the Prime Minister to review the list of operational purposes annually, which occurred in August 2025.

Home Office Handling Arrangements

- 3.24 In autumn 2024, we were made aware by the Home Office that the recently appointed Home Secretary had not yet reviewed and approved the Handling Arrangements for the treatment of material gathered under IPA warrants. The then Home Secretary had received a verbal briefing on her responsibilities relating to IPA warrants on the day she was appointed, which covered the existence of these Handling Arrangements and advice from senior officials in the Home Office (who had reviewed them in detail) that they were confident the arrangements were satisfactory. The Home Office initially added a form of words to warrant submissions to remind the Home Secretary that she must be personally satisfied there are satisfactory handling arrangements. They intended to include this form of words until she had personally reviewed the full detail of the Handling Arrangements.

- 3.25 During the Home Office inspection held in December 2024, it became apparent that the form of words added to warrant submissions had mistakenly fallen out of use and that the detail of the Handling Arrangements had still not been personally reviewed by the Home Secretary. We issued an action for the Home Office to rectify this urgently and write to us to confirm it had completed the action.
- 3.26 The Home Secretary personally reviewed the full detail of the Handling Arrangements in March 2025, eight months after taking office. The IPA requires the Home Secretary is personally assured that satisfactory handling arrangements are in force.¹⁴ The Home Office considers that a Home Secretary may be so satisfied on the basis of advice from senior officials, who had reviewed the detail of the Handling Arrangements, in their consideration of whether they are satisfactory. However, we consider that it is hard to see how the then Home Secretary can have reached such a conclusion that took into account all relevant considerations without having considered the detail of the handling arrangements and without offending the principle against sub-delegation.
- 3.27 We are satisfied that the situation was resolved as of March 2025 and acknowledge the work the Home Office have done to improve its initial inductions of new Home Secretaries going forwards. We note that questions relating to the consistency of such approaches with public law principles are, where necessary, matters for determination by the courts.

Target discovery misidentification

- 3.28 During 2025, GCHQ reported an issue where, in the context of target discovery work, it had misidentified selectors in a small number of cases that were wrongly suspected of being involved in terrorism-related criminality. The issue arose in connection with a particular software application, which was one of a class of internet applications used by a relatively small section of the public. However, this particular application operated in an unusual way which meant, unbeknownst to GCHQ, that the target discovery methodology was unreliable. With the advice of the Technology Advisory Panel (TAP), IPCO officials robustly challenged whether GCHQ, given its vast technical expertise, could, or should, have identified the unusual way in which the specific application operated, but we ultimately concluded this was not foreseeable.
- 3.29 Unfortunately, the misidentified selectors were provided to the police and resulted in some executive action, including five port stops under Schedule 7 to the Terrorism Act 2000, being taken against members of the public who were later identified as not being involved in the suspected criminality. Our subsequent detailed investigation identified that although inaccurate intelligence had been disseminated, there had not been a relevant error, as defined by the IPA. This is because the activity was lawfully authorised under an interception warrant and the adoption of an unintentionally and unforeseeably imperfect target discovery methodology did not constitute such an error. Notwithstanding the categorisation of the incident, there had been serious prejudice caused to the people concerned: but for the inaccurate intelligence, these individuals almost certainly would not have been subjected to a port stop (i.e., detained, had their electronic devices downloaded and biometrics taken).
- 3.30 Had we determined that a relevant error had occurred, we would have begun consideration of whether this constituted a "serious error". Section 231(1)(b) of the IPA enables the IPC to inform a person who is the subject of a serious error in certain circumstances, though in this case, this provision did not apply as the circumstances surrounding the

14 In the case of targeted interception warrants, see section 19(1)(c) and section 30(1)(a) of the IPA.

misidentification did not amount to a relevant error. We have reflected whether this incident engages issues under Article 13 European Convention of Human Rights (right to an effective remedy) given that there is no mechanism to inform an affected person in these circumstances. However, we have concluded that, although the impact on those affected is highly unfortunate and regrettable, intelligence can sometimes simply be wrong. In addition to protecting privacy and fundamental freedoms, it is in the interests of those agencies to ensure limited public resources are used efficiently to investigate genuine threats to national security.

- 3.31 The investigative measures taken in response to the incorrect intelligence in this case, including port stops by the police, were undertaken in good faith and were a reasonable response to possible terrorism-related criminality. It should be noted that port stops are controversial no-suspicion powers that can be used to stop any member of the travelling public without an intelligence case being needed. We are satisfied that neither GCHQ nor any other public authority, including the police, were at fault. We can also confirm that GCHQ acted to minimise the effects of these misidentifications as soon as it became aware of the issue. We will continue to keep target discovery operations under close scrutiny.
- 3.32 This was a serious matter that required careful consideration. It highlighted the inherent complexity of error investigations and the potential for significant prejudice or harm to be caused in circumstances that do not constitute a relevant error. Under section 231(9) of the IPA, the IPC is required to keep under review the definition of a relevant error and we will consider this issue as part of that work.

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

- 3.33 In December 2023, much of paragraph 62 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019 (Schedule 3) was repealed. This included the restriction on reporting on the IPC's functions under Schedule 3 in our main Annual Report. We therefore include below a summary of the functions exercised by Judicial Commissioners under Schedule 3, which have formed part of our work since Schedule 3 came into force in 2020.

Overview

- 3.34 Schedule 3 provides certain police officers, referred to as 'examining officers', with the power to stop, search, detain and question individuals at a UK port or in the Northern Ireland border area to determine whether they are, or have been, engaged in hostile activity. Paragraph 1(4) makes clear that the power to stop and question can be exercised "whether or not there are grounds for suspecting that a person is or has been engaged in hostile activity". Hostile activity, as defined in paragraph 1, has two elements:
- (i) a hostile act, which is an act which threatens national security or the economic well-being of the United Kingdom, or is an act of serious crime; and,
 - (ii) which is carried out for, on behalf of or otherwise in the interests of a State other than the United Kingdom.
- 3.35 Schedule 3 therefore affords similar powers to those under Schedule 7 of the Terrorism Act 2000, but is intended to operate against hostile state threats rather than terrorism. A Code of Practice has been issued by the Home Office in relation to the exercise of Schedule 3 powers by examining officers.¹⁵

15 See: Schedule 3 code of practice

IPC functions

- 3.36 Confidential material, including legally privileged and confidential journalistic material, is protected under Schedule 3 through a referral mechanism to the IPC. This requires that retention and use of an article, or a copy of an article which contains confidential material, must be authorised by a Judicial Commissioner.
- 3.37 Paragraph 11 of Schedule 3 allows an examining officer to retain articles found during a search or provided to them when an individual is questioned, for one or more specified purposes. Those purposes are set out at paragraph 11(2), and include retention while the officer believes that an article could be used in connection with the carrying out of a hostile act, or while necessary to prevent death or significant injury.¹⁶ Where an article is retained on either of those grounds, the case must be referred to the IPC. A Judicial Commissioner must then decide whether to authorise the retention and use of the article, with additional requirements if that article contains or includes confidential material. If retention is not authorised, the Judicial Commissioner must direct that the article is either destroyed or returned to the person from whom it was taken.¹⁷
- 3.38 Similarly, under paragraph 17 of Schedule 3, an examining officer may make and retain a copy of any article they find or receive during a Schedule 3 stop. When that copy contains confidential material, and it is retained because the examining officer believes it necessary in the interests of national security or the economic well-being of the UK, for the purpose of preventing or detecting serious crime, or to prevent death or significant injury, the case must be referred to the IPC. Paragraph 18 requires a Judicial Commissioner either to approve retention and use of a copy, which may be subject to any conditions the Commissioner thinks appropriate, or to order its destruction.

Process

- 3.39 Before a Judicial Commissioner makes a decision under either paragraph 12 or paragraph 18, we must seek representations from the affected parties. These include the person from whom the article was taken and/or copied, the Home Secretary, and the responsible chief police officer, who is ordinarily the Commissioner of Police of the Metropolis. These representations are usually sought sequentially, with seven days allowed by the IPC for each stage. In the case of both articles and copies, Schedule 3 also provides for an urgent procedure requiring representations to be exchanged and a decision taken within a much shorter prescribed timeframe.
- 3.40 Once representations have been received, or the prescribed deadline has passed, a Judicial Commissioner considers the case and decides whether to authorise retention. That decision is provided in writing to the affected parties.
- 3.41 Schedule 3 allows affected parties to ask the IPC to decide whether to approve the way in which a function was exercised by a Judicial Commissioner. The IPC approaches this as a substantive right of appeal, rather than a review, meaning further evidence can be considered and the decision is taken afresh.

¹⁶ See: paragraph 11(2)(d) and (e) of Schedule 3.

¹⁷ See: generally, paragraph 12 of Schedule 3.

Omagh Bombing Inquiry

- 3.42 During 2024 and 2025, we received and complied with three requests in relation to the Omagh Bombing Inquiry pursuant to rule 9 of the Inquiry Rules 2006. These requests related to potential material IPCO, or one of its precursor organisations,¹⁸ may have held that was of relevance to the Inquiry's Terms of Reference.¹⁹ We have complied with these requests and continue to provide assistance to the Inquiry as required.

Raising concerns with IPCO

- 3.43 As set out in our "Disclosing Information to IPCO" guidance,²⁰ section 237 of the IPA provides an information gateway for anyone, including current and former employees of the public authorities which we oversee, to raise with us any serious concerns they have.
- 3.44 In 2025, we received five new disclosures of information. Two of these related to an LEA where the IPC concluded that, following an investigation, there was no evidence of non-compliance. In the third case, which also related to an LEA, we were not provided with sufficient information to commence an investigation and the matter was therefore closed. The fourth case related to an approach taken by an LEA, which the IPC concluded was in compliance with the law.
- 3.45 The fifth case related to the CHIS handling structure at a government department. Following investigation, the allegations were substantiated and the individual was informed of the outcome.
- 3.46 In our 2024 Annual Report, we reported a case relating to a disclosure about HMPPS. In 2025, we concluded this investigation and found that a relevant error had occurred.

Vetting arrangements

- 3.47 All Inspectors are vetted to the appropriate National Security Vetting level by UK Security Vetting. In 2025, we engaged with a public authority under our oversight regarding separate additional security checks being applied to our Inspectors prior to the public authority granting access to its premises for the purpose of conducting inspections.
- 3.48 Section 235(3) of the IPA places all public authorities overseen by the IPC under a legal obligation to provide such assistance that the IPC may require. Section 235(4) clarifies that this may include access to necessary facilities. The IPC considers that the imposition of bespoke vetting arrangements on IPCO staff is inconsistent with maintaining IPCO's independence. Even if implemented with the best of security intentions, it would effectively provide that public authority with a veto over who conducts its inspection. The checks were implemented without any prior discussion and without any recognition of the potential implications. It is not acceptable for any public authority to decide which of our Inspectors should inspect it and it is for this reason that the Cabinet Office previously

18 The previous organisations were the Office of Surveillance Commissioners (OSC), the Interception of Communications Commissioner's Office (IOCCO) and the Intelligence Service Commissioner's Office (ISComm).

19 See: Omagh Bombing Inquiry Terms of Reference – Omagh Bombing Inquiry

20 See: Disclosing-information-to-IPCO.pdf

concluded that both internal and external candidates for roles at IPCO should have access to an independent appeal mechanism (i.e., the Security Vetting Appeals Panel) for adverse vetting decisions (see our previous annual reports for further information).²¹

- 3.49 In October 2025, the IPC wrote to the Home Office and the relevant public authority to set out our position. In response, the public authority relented and IPCO inspectors have now been exempted from these additional security checks.

21 Annual Report of the Investigatory Powers Commissioner 2022 (from paragraph 3.10). See: Annual Report of the Investigatory Powers Commissioner 2022. Annual Report of the Investigatory Powers Commissioner 2023 (paragraph 2.22). See: Annual Report of the Investigatory Powers Commissioner 2023

4. Oversight activities and challenges

Summary

- 4.1 This chapter presents our oversight findings and emerging challenges which have been identified from our inspections and authorisations work during the 2025 reporting year.
- 4.2 Below is an overview of chapter 4, along with a guide on how to navigate the chapter:

How to navigate this chapter



To help readers access relevant content quickly, the chapter has been structured as follows:

Our Inspections

- 4.4 UK intelligence community (UKIC)
- 4.6 Law enforcement agencies (LEAs)
- 4.7 Wider public authorities (WPAs) and local authorities
- 4.10 Prison services

Regulation of Investigatory Powers Act 2000 (RIPA)

- 4.12 Covert human intelligence sources (CHIS)
- 4.33 Directed surveillance

Investigatory Powers Act 2016 (IPA)

- 4.35 Bulk interception
- 4.39 Targeted interception (TI) and targeted equipment interference (TEI)
- 4.56 Communications data (CD): LEAs, public authorities and prisons
- 4.57 Records and Product Management (RPM)

UK-US Data Access Agreement (DAA)

- 4.69 Overview
- 4.74 Crime (Overseas Production Orders) Act 2019 (COPO)

The Principles

- 4.76 Key findings
- 4.81 Review of The Principles

The Equities Process

- 4.83 Key findings

Our inspections

- 4.3 Detailed below is a summary of the most significant compliance matters identified during our inspections in 2025. These issues are considered sufficiently material to warrant inclusion in this Annual Report. Following this summary, each area is set out in greater detail to provide further context and insight into our inspection findings.

UK intelligence community (UKIC) and warrant granting departments (WGDs)

- 4.4 During 2025, we continued to inspect each of the UK intelligence agencies (MI5, the Secret Intelligence Service (SIS), Government Communications Headquarters (GCHQ), the Ministry of Defence (MoD) and warrant granting departments (WGDs)) across the full range of their covert investigatory powers. The inspection programme is subject to adjustment each year as the use of powers and compliance levels change or as new legislative developments occur. This can mean that Inspectors will review the use of some powers more than once a year.
- 4.5 Key areas covered in this chapter include:
- **Access to records and inspection methodology:** changes to how we select and access MI5 covert human intelligence source (CHIS) records, following learning from our 2022 Agent X inspection report and a pilot approach in 2025. [See: paragraphs 4.12–4.14].
 - **Risk management for CHIS overseas:** ongoing concerns around the standard of MoD CHIS risk assessments, including an error relating to the welfare and security of one of its CHIS. [See: paragraphs 4.15–4.18].
 - **International data sharing:** During our 2025 inspection, we found that GCHQ had appropriate safeguards of confidential information resulting from bulk interception for its own analysts but raised significant concerns about whether overseas partners were complying with enhanced protections for journalistic and legally privileged material. [See: paragraphs 4.35–4.38].
 - **Safeguarding and records management:** continued concern about GCHQ's work to locate and account for removable media potentially containing IPA-related data. [See: paragraphs 4.66–4.68].

Inspections

2025 at a glance

426

In 2025, our Inspectors conducted 426 inspections, fulfilling our statutory duty to oversee investigatory powers.



Inspection activity categorised by organisation type

Each team visit counts as one inspection. Organisations can be inspected multiple times a year by different teams, depending on the investigatory powers in use. Where police forces in England and Wales collaborate regionally, we conduct regional inspections to ensure proper use of covert powers.

● Police and law enforcement agencies	170
● Local authorities	114
● Prisons	46
● Intelligence agencies (+ MoD)	38
● Warrant granting departments	5
● Other (all other public authorities)	53

Law enforcement agencies (LEAs)

- 4.6 LEAs remained a major focus of our inspection programme in 2025. We reviewed their use of a wide range of investigatory powers under both RIPA and the IPA. The more significant findings and issues are set out in the sections that follow. In particular:
- **TEI:** an overall improving picture, but continuing issues for some LEAs in drafting warrants and a widening gap between authorities with mature regimes and those without. [See: paragraphs 4.54–4.55].
 - **CD:** most public authorities generally maintain high standards when exercising their power to acquire CD, with non-compliance mainly occurring in urgent authorisations and Single Point of Contact (SPoC) gatekeeping. [See: paragraph 4.56]
 - **National Crime Agency (NCA) operational records:** a compliance issue on demonstrating lawful review, retention and disposal of CHIS, undercover and RIPA-related material across electronic and hard copy holdings. [See: paragraphs 4.64–4.65].

Wider public authorities (WPAs) and local authorities

- 4.7 Local authorities in the UK have access to a limited set of investigatory powers, specifically the use of CHIS, directed surveillance and the acquisition of CD. These powers are generally low volume activity. Since 2023, we have operated a risk-based inspection model, requiring written assessments of compliance to determine whether remote or in-person inspections are necessary.
- 4.8 WPAs, which include various organisations beyond local authorities, also hold statutory powers to use covert tactics. The scope of these powers varies depending on the organisation's functions, with many authorised to conduct directed surveillance and acquire CD, while only a few can use methods like property interference and intrusive surveillance. Local authorities may acquire communications data only through collaboration arrangements certified under the IPA and, in practice, through membership of the National Anti-Fraud Network (NAFN).
- 4.9 Inspection intervals depend on how frequently the bodies use their powers, ranging from once a year to every three years. In 2025, we conducted 53 inspections of WPAs and 114 inspections of local authorities. Overall, we observed high levels of compliance, and no instances of non-compliance or concerns requiring formal inclusion in this Annual Report were identified.

Prison services

- 4.10 In 2025, our prison oversight focused on whether interception and monitoring arrangements are being applied lawfully, consistently and with the safeguards required by the relevant legal and policy frameworks. Key areas covered in this chapter include:
- **Interception by His Majesty's Prison and Probation Service (HMPPS):** inspections of interception and monitoring practices across the HMPPS prison estate revealed recurring compliance issues with the Prison Rules and the Authorised Communications Controls and Interception Policy Framework (ACCIPF). [See: paragraphs 4.41–4.44].
 - **Secure Training Centres:** continuing concerns about the legal basis relied on for interception (rule 10 of the STC Rules 1998), including the absence of explicit necessity/proportionality tests and protections for confidential/legally privileged communications. [See: paragraphs 4.45–4.48].

- **Interception in the Scottish Prison Service (SPS):** we continue to work constructively with SPS to address areas of concern identified across policies, processes and operational practices following the December 2024 thematic inspection. However, we are concerned that some recommendations remained at an early stage of implementation. [See: paragraphs 4.49-4.53].

Regulation of Investigatory Powers Act 2000 (RIPA)

- 4.11 RIPA provides a framework for the lawful use of surveillance CHIS by public authorities in the UK.²² We oversee the exercise of these powers to ensure they remain necessary, proportionate and compliant with the law.

Covert human intelligence sources (CHIS)

Access to MI5 CHIS records

- 4.12 Our inspections of CHIS at MI5 have been complex, largely due to how material is stored and accessed. We reviewed a selection of cases at each inspection, based on identified risk factors and random sampling. Relevant material is held across two separate IT systems which are not designed to give Inspectors direct access without exposing highly sensitive operational detail. MI5 therefore transfers material it considers relevant into a secure review environment. This has meant we have not always been confident that the material provided reflects the full set of factors informing compliance decisions. While MI5 responds to requests for further records, Inspectors can only request additional material where its existence is apparent from what has been provided.
- 4.13 IPCO and MI5 recognised these limitations and agreed a revised approach for our 2022 inspection of the Agent X case. A significantly greater proportion of the CHIS record was made available at the outset, including material from both primary systems. This provided a fuller view of decision-making and identified relevant material that had not routinely been included in inspection packs. As set out in our 2022 report, we made a number of compliance findings on the adequacy of MI5's CHIS record-keeping.²³ We have since continued to work with MI5 to improve how CHIS records are selected and made accessible for inspection.
- 4.14 Following further discussion, we piloted a revised approach at a September 2025 inspection, whereby Inspectors first reviewed core documents across a wider set of CHIS cases before selecting cases for full examination, at which point the entire record was made available. This has improved our understanding of how MI5 manages CHIS records and mitigates risks relating to individual sources. We have adopted this approach for all MI5 CHIS inspections and will keep it under review to ensure it continues to provide appropriate access to material.

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

23 See: paragraph 5.4.

MoD CHIS compromise and error

- 4.15 In 2023, the MoD introduced a policy to authorise all CHIS under RIPA, regardless of location. While the statutory requirement applies only to CHIS activity in the UK or with a UK connection, this change coincided with our oversight of MoD CHIS and surveillance activity overseas being placed on a statutory footing.
- 4.16 Since 2021, we have identified repeated non-compliance in the standard of MoD CHIS risk assessments, including cases where assessments did not adequately address the risks faced by CHIS operating in hostile environments.
- 4.17 In January 2025, we were notified of an administrative error in a CHIS case involving a serious operational security compromise. Our subsequent inspection identified further significant compliance concerns, and a focused inspection in December 2025 found serious failings in case management and wholly inadequate risk assessments. The MoD accepted these findings and reported the matter to us as a relevant error.
- 4.18 Following the compromise, the Chief of Defence Intelligence commissioned a comprehensive internal review of MoD CHIS policy and practice. All recommendations were accepted and the MoD has begun a wide-ranging programme of improvement. We consider this action necessary and reassuring and will continue to monitor progress, reporting further in our 2026 Annual Report.

Juvenile CHIS

- 4.19 Juvenile CHIS authorisations remain rare, are granted only in exceptional circumstances and are subject to additional oversight. This is demonstrated by the fact that only one Juvenile CHIS was authorised by LEAs in 2025. We have covered details of this case in the Errors and Breaches chapter as the Investigatory Powers Commissioner (IPC) was not notified of this authorisation within the required seven-day period set out in the CHIS Code of Practice 2022.²⁴

Criminal Conduct Authorisations (CCAs)

- 4.20 Through our inspections, we identified recurring deficiencies in the preparation and oversight of Criminal Conduct Authorisations (CCAs), including for relevant sources (undercover operatives). The most persistent issue was how authorised criminal conduct was articulated, with applications often relying on generic or templated wording rather than clearly defining the specific conduct required. This falls short of the statutory requirement for conduct to be bespoke, tightly bounded and justified on its own merits, in line with RIPA and the revised CHIS Code of Practice 2022.
- 4.21 We also found inconsistencies in proportionality assessments, with some authorisations relying on broader operational context rather than addressing directly why the conduct itself was necessary and the least intrusive means available. In addition, we identified instances where review periods for CCAs and related section 29 authorisations were not aligned, undermining coherent oversight.
- 4.22 We emphasised the need for more rigorous authorisation and management of CCAs, including clearly defined permissions and limitations, effective communication to CHIS, and complete and accurate record keeping. Particular care is required where thematic CCAs are used, to ensure eligibility is properly identified and kept under review.

24 See: paragraph 7.23-7.24

- 4.23 While there were examples of well-constructed authorisations, these findings highlight the need for greater consistency, stronger supervisory oversight and closer adherence to the statutory framework, to ensure the safeguards intended by Parliament are met.

HMPPS CHIS non-compliance

- 4.24 During our 2025 inspection, we identified two areas of critical non-compliance:
- First, HMPPS did not consistently apply the Chapter 9 Safeguards of the CHIS Code of Practice 2022 weakening the protections therein. We found that some practitioners lacked sufficient understanding of the importance of these safeguards.
 - Second, the systems and procedures used by HMPPS at one prison to manage covert activity have not consistently aligned with HMPPS policies and structures. This issue, which we have examined over several years, still has not been resolved. CHIS Handlers and Controllers are being managed by Prison Managers and fall ultimately under the authority of the Governor, rather than being overseen within the Regional Intelligence model.
- 4.25 We found CHIS applications and authorisations to be of a consistently good standard, supported by effective Authorising Officer oversight, clear records and appropriate use of policy logs. While findings were largely positive, we identified minor areas for improvement. In several cases, applicants relied on generic wording to describe security risks within the prison environment and cited cost or resource savings to support proportionality. Such considerations are of very limited weight to the RIPA proportionality assessment in this context.
- 4.26 We were pleased to see HMPPS had strengthened its approach to managing the risk of CHIS “status drift” through the introduction of a new IT system.²⁵ We found that prisons actively monitor status drift registers and that policies and procedures were applied effectively, mitigating the risk of inadvertent CHIS activity and supporting the appropriate identification of intelligence opportunities.
- 4.27 In summary, while recent enhancements have bolstered the management of status drift and improved compliance in this area, critical issues remain. Robust systems and a deeper awareness among practitioners are essential to safeguarding requirements. CHIS activities generally demonstrate sound practice, yet minor procedural lapses indicate room for refinement.

Thematic inspection of relevant source activity

- 4.28 Our findings and recommendations confirmed that the undercover community continued to demonstrate a high level of professionalism and commitment, underpinned by well-trained operatives and experienced management and oversight structures across the UK. We observed a strong emphasis on compliance throughout the thematic inspection and the associated nine-month programme of oversight. This was reinforced by the constructive and timely way in which the community responded to issues identified by Inspectors and recommendations made in the report. Many of these issues have been resolved promptly, while others will take longer and remain under review.

25 Status drift refers to failures to identify and properly authorise the use and conduct of a source when the nature of their reporting brings them within the statutory definition of a CHIS.

- 4.29 We found that communication between us and the relevant national undercover organisations remained effective, enabling concerns to be raised and resolved efficiently. The IPC discussed and endorsed the findings of the thematic inspection directly with the Chair of the National Undercover Working Group, Chief Constable Trevor Rodenhurst KPM.
- 4.30 The inspection identified areas where further improvements would strengthen consistency, oversight and compliance in relation to relevant source activity. Greater standardisation of IT systems, documentation and decision-recording practices would support a more uniform approach across units. We also identified scope to enhance the quality and professionalism of applications, including using specialist applicants, clearer authorisation parameters, accurate renewal recording and more robust assessments of proportionality.
- 4.31 We considered that governance and assurance would be further strengthened through regular reviews by Operational Security Advisors and clearer oversight by Senior Responsible Officers (SRO). We also identified opportunities to enhance professional development, including re-accreditation arrangements for infrequently deployed SRO and the establishment of a national peer support network to promote consistency and the sharing of good practice.
- 4.32 In addition, we emphasised the importance of maintaining robust welfare documentation, managing collateral intrusion carefully and ensuring that CCAs were limited to those permitted under section 29B. Updating National Undercover Working Group guidance would help ensure that operational practice remained aligned with legislative developments and evolving operational requirements.

Directed surveillance

HMPPS

- 4.33 We found that directed surveillance applications and authorisations were generally well drafted, with appropriate consideration of proportionality and collateral intrusion. However, some proportionality submissions were unclear or included information not relevant to the Code of Practice. References to public expectations of covert tactics were misplaced and do not diminish an individual's right to privacy. Proportionality assessments must instead focus on minimising intrusion. Authorising Officer rationales were largely clear, though in one operation overly broad wording risked capturing innocent third parties. Surveillance activity should be more precisely defined and restricted to individuals criminally linked to the subjects.

Investigatory Powers Act 2016

- 4.34 The IPA provides a comprehensive framework for the use of investigatory powers by law enforcement and intelligence agencies. It consolidates and updates previous legislation, establishing safeguards and oversight mechanisms for the use of interception, equipment interference, CD acquisition and bulk powers. We oversee the use of these powers to ensure they are used lawfully, proportionately, and in accordance with the safeguards set out in the Act.

Bulk interception

Additional safeguards of confidential information resulting from bulk interception

- 4.35 During our bulk interception inspection of GCHQ in early 2025, we explored compliance with the enhanced safeguards for confidential journalistic material and material identifying journalistic sources introduced in April 2024 by The Investigatory Powers Act 2016 (Remedial) Order 2024 (see section 154 of the IPA).²⁶ These changes introduced a requirement for prior judicial authorisation where the purpose of querying bulk interception product (i.e., selection for examination) is to identify such material or where this is highly likely.
- 4.36 While we were satisfied that GCHQ had implemented appropriate guidance and governance to secure compliance with this requirement in respect of its own analysts, the inspection gave rise to significant concerns as to whether GCHQ had ensured that there were adequate arrangements in place to secure compliance in respect of overseas partners which have access to GCHQ's unselected bulk interception product. These concerns extended more widely to the equivalent arrangements to secure compliance with the enhanced safeguards for the sharing of legal privilege material in section 153 of the IPA and whether GCHQ had sufficient visibility of search term query errors made by overseas partners in respect of product selected under its own warrants.
- 4.37 We required GCHQ to review the arrangements it has in place with all overseas partners which have access to GCHQ unselected bulk interception product. This was a major workstream that required GCHQ to review and engage with partners, all of whom have varying systems, processes and domestic legal frameworks. The initial review was completed by GCHQ in December 2025 and shared with IPCO. The review provided assurances that, in general, controls were in place to either prohibit overseas partners' acquisition of material covered by IPA enhanced safeguards or to provide a mechanism to comply with sections 153 and 154 of the IPA via liaising with GCHQ. However, the review indicated that inadequate arrangements in respect of journalistic material subsisted in respect of a major overseas partner, but both GCHQ and the partner were committed to resolving this. The review revealed surprisingly low instances of partners requesting permissions under sections 153 and 154 of the IPA via GCHQ and exploring this further will be a focus of IPCO inspection activity in 2026.
- 4.38 We outlined our concerns with our overseas counterparts through our international engagement work in 2025 and it was agreed to explore further the extent to which mutual assurance could be provided for international sharing arrangements between SIGINT agencies.²⁷ We will seek to revisit this during future international engagement activity, including through the Five Eyes Oversight and Review Council (FIORC).²⁸ We will update on this issue in our 2026 Annual Report.

26 See: The Investigatory Powers Act 2016 (Remedial) Order 2024

27 Signals Intelligence (SIGINT) refers to the collection and analysis of data derived from signal transmissions, such as communications and electronic signals.

28 The Five Eyes is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States of America.

Targeted interception (TI)

IT system for the management of intercept material

- 4.39 In July 2024, the Home Office announced that it would no longer deliver a system to replace the ageing platform used by LEAs to manage their interception capability and intelligence product; this will now be replaced by four bespoke solutions developed by the interception LEAs themselves with some support from the Home Office. We have continued to monitor these developments closely via attendance at monthly Targeted Interception Service Programme (TISP) meetings. While we remain concerned about ensuring the solutions are compliant with the IPA, it is noted that the Home Office's will continued to provide 3rd line support of the legacy system while the new platforms are in development.
- 4.40 The current IT system was originally scheduled to be decommissioned in September 2026. Three of the TI LEAs are satisfied that their new solutions will be operational by this date. However, the other two TI LEAs have already indicated that they will remain reliant on the existing system beyond this date. The Home Office has confirmed that they will continue to provide 3rd line support for as long as the LEAs require the service.

Interception: HMPPS

- 4.41 While our 2025 inspections of interception and monitoring practices across the HMPPS prison estate identified some examples of good practice, they continued to reveal recurring compliance issues when assessed against the Prison Rules and the ACCIPF.
- 4.42 We identified significant inconsistencies in operational practices throughout the estate. These issues were further intensified by a lack of clarity regarding ACCIPF requirements, as inspection outcomes highlighted ongoing ambiguity within the policy framework and associated operational guidance, which impeded both compliance and effective oversight. Inspectors frequently encountered uncertainty surrounding authorisation protocols, error reporting procedures, and the management of intercepted material, reinforcing the need for a unified, transparent and consistently implemented framework.
- 4.43 In August 2025, the IPC formally raised these concerns with HMPPS senior leadership. HMPPS acknowledged the severity of the issues identified and committed to a series of workstreams intended to address non-compliance. These included the publication of interim guidance pending a full policy review, the establishment of an Interception Assurance Team, and a comprehensive review of the ACCIPF, with publication anticipated in late 2026.
- 4.44 While the IPC acknowledged the commitments undertaken by HMPPS, substantial improvement remains necessary. We maintain oversight through inspection activities and ongoing engagement with senior HMPPS leadership to evaluate whether the implemented measures effectively ensure lawful, consistent and proportionate interception and monitoring practices.

Interception: Secure Training Centres

- 4.45 Secure Training Centres (STC) form a distinct part of the youth custodial estate and operate under a separate legislative framework from both adult prisons and Young Offender Institutions (YOIs). At present, only one STC is in operation in the United Kingdom.

- 4.46 Our 2025 inspections continued to highlight concerns, first identified in 2024, regarding the ambiguity of rule 10 of the STC Rules 1998, relied on as the legal basis for the interception of trainees' communications.
- 4.47 In practice, internal procedures at the STC broadly mirror those applied across the wider custodial estate and we found no evidence of unnecessary or disproportionate monitoring. However, these procedures are local in nature and are not supported by the statutory safeguards found elsewhere. Unlike equivalent rules governing adult and youth establishments, rule 10 contains no tests of necessity or proportionality, and provides no explicit protections for confidential or legally privileged communications.
- 4.48 We have significant concerns as to whether rule 10 complies with the European Convention on Human Rights (ECHR) requirements and continue to engage closely with the Youth Custody Service to ensure that legislative and procedural reforms are progressed without further delay.

Interception: Scottish Prison Service (SPS)

- 4.49 During 2025, the SPS engaged constructively with our oversight following the thematic inspection issued in December 2024 on compliance with section 49 of the IPA. The SPS set out a programme of work to address concerns across policy, process and operational practice.
- 4.50 We have seen early progress, including steps to improve consistency and transparency across the estate. This includes proposals to standardise how prisoners are informed of monitoring, strengthen the recording of justifications for interception, reinforce requirements around exempt communications and revise public information to make clear that general correspondence may be monitored.
- 4.51 However, several recommendations remain at an early stage. These include the review of phone monitoring processes and the introduction of formal authorisation, review and cancellation arrangements. We also identified weaknesses in the handling of general correspondence, with the SPS recognising the need for more consistent and auditable processes for justifying interception. Work is ongoing to review local practices and develop a more consistent national approach.
- 4.52 In January 2026, the IPC formally acknowledged SPS's response and welcomed the actions proposed, while emphasising the need to maintain momentum and deliver these consistently across the estate. We will support this through dip-sampling inspections of selected prisons in 2026, ahead of a full inspection programme in 2027. One of our Judicial Commissioners leads on Scottish prisons and, in common with other areas we oversee, will assist with inspections during 2026.
- 4.53 We will continue to monitor progress and assess the effectiveness of these measures and will report further in our 2026 Annual Report.

Targeted equipment interference (TEI)

- 4.54 During our 2025 inspections, we assessed the overall use of TEI by LEAs as improving. However, a number of issues identified in our 2022 thematic review remain. We also observed a growing disparity between those authorities with structured and compliant regimes and those where understanding and application of the warrant process remains underdeveloped. While this often reflects frequency of use, performance among larger

LEAs is not uniform. In particular, some continue to encounter difficulty in constructing warrants, including the use of instruments and schedules, and accurately identifying and describing the relevant section 101(1) subject matter in line with section 115(3) of the IPA.

- 4.55 As the use of more complex TEI techniques increases, we expect this disparity to widen. This raises questions about the sustainability of the current model, under which all police forces maintain independent TEI capability. In our view, greater consistency and compliance will depend on cross-organisational collaboration and the development of a more unified approach. We will continue to encourage alignment across LEAs, including through engagement with the Home Office in the context of proposals for a National Police Service.

Communications data (CD)

- 4.56 Overall, we found that public authorities exercised their power to acquire CD at a consistently high standard. We identified that most areas of non-compliance related to urgent authorisations and Single Point of Contact (SPoC) gatekeeping, where records sometimes failed to show that designated senior officers exercised effective control or demonstrated adequate understanding. We also observed variable standards in application quality, particularly around the justification of necessity and proportionality, the assessment of collateral intrusion and allocation of priority grading, which indicated an ongoing reliance on individual expertise rather than consistently embedded assurance processes.

Records and Product Management (RPM)

- 4.57 The IPA requires all public authorities to have satisfactory arrangements in place to protect material obtained through the exercise of investigatory powers and to minimise unnecessary intrusion. This section sets out our oversight of how those arrangements are implemented in practice across the authorities we inspect.

LEA

- 4.58 Assessing compliance with the requirements to safeguard CD obtained under the IPA remained a key focus of oversight during 2025. Historically, this issue has presented considerable challenges for public authorities, primarily because responsibility for developing solutions was delegated to operational staff already coping with substantial workloads.
- 4.59 We have revised our inspection approach to provide a more proportionate and focused assessment that reflects learning from joint work with the Information Commissioner's Office (ICO) on governance, data protection and organisational accountability.
- 4.60 Inspections completed throughout the year showed that many organisations have strengthened their governance structures, with clearer lines of responsibility, improved senior oversight and more consistent processes for managing data. Staff understanding has generally improved through mandatory training and internal guidance, although the availability of structured refresher training varies.
- 4.61 We observed improved use of basic records-management tools designed to map what information organisations hold, how it is used and who is responsible for it. However, these records were not always comprehensive or regularly reviewed. Information risk and

security arrangements were generally robust, but continued reliance on manual steps, such as identifying review dates, recording decisions and deleting records, still creates risks of over retention or delay.

- 4.62 Further progress is needed to automate these processes, particularly within commonly used systems. Internal assurance arrangements also varied, with some organisations relying on informal or infrequent checks rather than a structured programme of review.
- 4.63 Looking ahead to 2026, inspections will continue with a stronger emphasis on organisations demonstrating effective internal audit and self-assessment arrangements as key indicators of sustained compliance and proactive risk management.

NCA

- 4.64 During our 2025 CHIS and surveillance inspection of the NCA, we identified a compliance issue in relation to its management of operational records. We found the NCA was unable to demonstrate consistently that CHIS, undercover and other RIPA-related material, held in both electronic systems and hard-copy records, was being reviewed, retained or disposed of in accordance with legislative requirements and relevant Codes of Practice. Significant volumes of records were held beyond their scheduled review dates and weaknesses in management information, particularly for hard-copy holdings, meant that material could not always be reliably linked to specific operations or subjects of interest.
- 4.65 These deficiencies limited assurance over the lawfulness, necessity and proportionality of continued retention and highlighted systemic weaknesses in governance and oversight, requiring formal remediation. The NCA recognises the issue and are seeking to address it: we will continue to keep this matter under review.

UKIC

- 4.66 In our 2024 Annual Report, we reported on the ongoing efforts by GCHQ to identify the location of and recovery of removable media, some of which may contain IPA-related data. These efforts continued during 2025 and GCHQ has written to the IPC to provide a detailed account of where it has got to with this work, and the action it has taken or plans to take to locate and recover these items.
- 4.67 The term removable media relates to such items as USB sticks, external hard drives, compact discs, memory cards and other portable media storage devices. These items are utilised extensively and are an essential component of some of GCHQ's operating processes. GCHQ has now scoped the extent of the issue in terms of the maximum number of items of removable media that it cannot immediately locate and are therefore unaccounted for. This is a very significant number, which GCHQ currently estimate to be in the thousands, and there is a programme of further work to locate and account for as many of these devices as possible. Once that work is complete, GCHQ will be able to report how many devices have been confirmed as lost.
- 4.68 We remain very concerned about this issue and are disappointed with the time it has taken GCHQ to investigate. GCHQ has recognised the importance of setting up a long-term solution to reduce the loss of removable devices. It has therefore commissioned a new tool for monitoring the issue, storage and location of removable media, which will come into use in 2026. We will continue to monitor GCHQ's progress in bringing this issue to a conclusion, both through our regular inspection activity and by requiring regular written progress reports from the organisation throughout 2026.

UK-US Data Access Agreement

- 4.69 Utilisation of the UK-US Data Access Agreement (DAA) by the intercepting agencies continues to grow and has become a vital part of both law enforcement and UKIC capabilities to counter serious criminal activities. During 2025, we continued to work positively with intercepting agencies to refine our inspection of their use of the DAA and have observed a notable improvement across the board. This included MI5, who we wrote to in 2024 about concerns that insufficient consideration was being given to the proportionality of targeting factors that would invoke the DAA.²⁹
- 4.70 All intercepting agencies were advised to strengthen their proportionality statements by making explicit reference to data held by certain United States (US) telecommunications operators (TO) which may have exceeded the scope of the request, including in relation to the time period requested and the types of data returned. This is due to the inability of some operators to provide a more specific response, leading to unintended collateral intrusion. While this is undesirable, access to these datasets is controlled within intercepting agencies and they rely on analytical tradecraft and training to ensure staff are aware not to exploit any data for which there is no valid necessity and proportionality case. We have required that these issues be recorded and explicitly addressed in applications, particularly if any of the data expected to be obtained will include a period where the subject was a juvenile.
- 4.71 Intercepting agencies reported a small number of errors where data was requested but there was not a valid targeted interception warrant in place. This can occur either when a mistake has led to the wrong account being targeted, or when the correct account was not de-tasked successfully when the agency had no further need to intercept it.
- 4.72 We remain satisfied that the UK Designated Authority (UKDA) infrastructure, together with controls applied by intercepting agencies, ensures any DAA request is for the purpose of preventing, detecting, investigating or prosecuting serious crime. We have continued to challenge, where necessary, any less straightforward serious crime matters, for example those that take place within certain national security contexts where the link to a particular covered offence may be far from obvious. UKDA infrastructure also ensures that only types of data from providers that are valid under the treaty is sought.
- 4.73 The UK cannot intentionally use the DAA to target a US Government entity or "US Person" (US citizen or resident, unincorporated US association or US corporation), or a person located within the US, known in the treaty as a "Receiving Party Person" (RPP). We remain satisfied that there is a very low risk of non-compliance with this requirement. Intercepting agencies take their responsibility to avoid targeting an RPP very seriously and proactively check multiple data sources to ensure they are not targeting an RPP before a request for DAA data is made; in addition, diligent post-targeting monitoring and sampling of the received data is conducted to establish if unwittingly an RPP has been targeted.

Crime (Overseas Production Orders) Act 2019

- 4.74 Our oversight of the DAA extends to public authorities obtaining overseas production orders under the Crime (Overseas Production Orders) Act 2019 (COPo). COPo orders ordinarily will be approved by a Circuit Judge. In 2025, we inspected four issuing agencies

29 Annual Report of the Investigatory Powers Commissioner 2024 (from paragraph 4.87). See: IPCO Annual Report of the Investigatory Powers Commissioner 2024

responsible for the majority of orders submitted to UKDA. Overall, we found high levels of compliance with DAA requirements. Other issuing agencies submitted few or no requests and will be inspected once activity increases.

- 4.75 We observed strong levels of knowledge and engagement with DAA requirements across issuing agencies. Staff demonstrated a clear understanding of compliance obligations, supported by thorough pre- and post-targeting checks, which mitigated the risk of targeting US persons. No reportable breaches of this nature were identified. Robust procedures were in place for identifying and handling legally privileged material, including prompt quarantine and independent legal review.

The Principles

- 4.76 Our oversight of “The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees” (The Principles) continued throughout 2025. We assess compliance with The Principles framework through targeted agency specific inspections and, from 2025, a cross-Principles Partners thematic inspection.
- 4.77 This new inspection enabled us to compare how the Principles Partners applied the assessment framework when engaged with a particular country or region as we noted some apparent inconsistencies in risk assessments during individual inspections. We wanted to determine whether the six Principles Partners were providing advice which addressed the requirements of The Principles, and whether each Partner was proceeding on the basis of a consistent assessment of the risks to relevant Ministers. Following this inspection, we were satisfied that the apparent anomalies were entirely justified based on the case specific facts.
- 4.78 Through the totality of our Principles inspection activity we found that five of the six Principles Partners were able to demonstrate consistently a high degree of compliance both in the substance and application. The way in which The Principles are embedded and applied across these public authorities reflects a well-established and mature framework.
- 4.79 During both its thematic and focused inspection, the MoD did not demonstrate the same depth of understanding of The Principles or a comprehensive understanding of its extant authorisation. The MoD is the only Principles Partner which does not have a separate government department scrutinising and stress-testing its risk assessments before seeking Ministerial authorisation, and this showed in the quality of its submissions which were not of the same high standard as other Principles Partners.
- 4.80 We reflected this in the inspection report and have issued the MoD with actions to improve its compliance and ensure the MoD’s approach is more consistent with other Principles Partners. These include developing additional training in The Principles and closer engagement with the Principles Partner Team, a cross-agency team that provides assessments of the background Principles risks on a country-by-country basis. We will continue to engage with the MoD throughout 2026 and will report on progress in our 2026 Annual Report.

Review of The Principles

- 4.81 In our 2024 Report, we reported that the Cabinet Office was reviewing The Principles in accordance with the policy intention that it should be reviewed every five years.

- 4.82 As part of this review, the Cabinet Office sought the views of interested parties, including non-government organisations and academics, through a consultation process and roundtable discussions, which we also attended. We understand that the Cabinet Office is now working through final submissions and we will report on this further in our 2026 Annual Report.

The Equities Process

- 4.83 In our 2023 Annual Report, we discussed the Equities Process, run by GCHQ on behalf of government, and noted that we had recommended the Process be reviewed to ensure it took account of vulnerabilities acquired by law enforcement and wider government.³⁰
- 4.84 Since 2023, GCHQ has made significant progress in improving access to the Equities Process, particularly for law enforcement, though further work is ongoing to strengthen the Process more broadly. The 2025 Equipment Interference Code of Practice now also requires public authorities to engage with the Equities Process.
- 4.85 As changes are made to the way the Process operates, it is necessary for us to keep pace to ensure our level of oversight is maintained. To that end, we have liaised with GCHQ during 2025 to understand changes and discuss the best ways for us to engage and oversee the way it conducts the Process. There has been no change to the starting position, which is always that disclosing a vulnerability will be in the national interest, and we have no concerns about the way decisions have been reached regarding disclosure or retention of vulnerabilities.

30 Annual Report of the Investigatory Powers Commissioner 2023 (from paragraphs 6.75 and 8.28). See: Annual Report of the Investigatory Powers Commissioner 2023

5. Oversight activities and challenges: Agent X

Overview

- 5.1 This chapter sets out the role we have had and continue to have, in the oversight of the Agent X case. As noted in our 2024 Annual Report, the Investigatory Powers Commissioner (IPC) undertook to report further on this matter.
- 5.2 This chapter is structured as follows:
- our involvement before 2025 [see: paragraphs 5.3-5.10];
 - Divisional Court and Investigatory Powers Tribunal (IPT) judgments in July 2025 [see: paragraphs 5.11-5.14]; and
 - our ongoing work on the investigation that we were directed to undertake by the Prime Minister³¹ following the 2025 judgments [see: paragraphs 5.15-5.21].

31 See: IPCO receives Prime Ministerial Direction for Agent X investigation – IPCO

Background

What is the "Agent X" case?

In late 2021, the Attorney General sought an injunction to prevent the BBC from publishing a story which alleged that a person known publicly as 'X' was an MI5 covert human intelligence source (CHIS) and reported a number of serious allegations against him, including that 'X' had used his status as an MI5 CHIS as a tool in abusing his partner. During those proceedings in the High Court, MI5 provided evidence stating that X's status as a CHIS had not been disclosed to the BBC. The injunction was granted which meant that while the BBC was able to report its story, it could not reveal X's identity.

Similar evidence was relied on by MI5 in separate proceedings in the IPT, responding to a claim brought by a person known publicly as 'Beth'. The IPT allowed MI5 to 'neither confirm nor deny' (NCND) whether X was a CHIS in those proceedings. 'Beth' sought judicial review of that decision, and MI5 maintained the position in that judicial review that X's status had not been disclosed to the BBC.

There were accordingly three sets of court proceedings relating to 'Agent X':

- (i) the injunction proceedings;
- (ii) 'Beth's' claim before the IPT; and
- (iii) 'Beth's' judicial review of the IPT's decision regarding NCND.

It became clear in late 2024 that MI5's position was incorrect, and that X's CHIS status was in fact confirmed to a BBC journalist by an MI5 officer in June 2020. MI5 corrected the false evidence before the High Court and the IPT. The IPC was directed by the Prime Minister to investigate how false evidence came to be provided, as discussed further below.

IPCO involvement before 2025

- 5.3 In January 2022, MI5 wrote to us about the BBC's interest in 'Agent X'; it stated that the BBC was seeking to disclose Agent X's role as an MI5 CHIS publicly, and shared a summary of allegations made by the BBC concerning Agent X. MI5 also indicated that it might seek an injunction to prevent the public disclosure.
- 5.4 In May 2022, Inspectors conducted an initial review of the case and found potential compliance issues requiring further investigation. The IPC wrote to MI5 in June 2022 requesting MI5 make available all records related to X for inspection, and in August 2022 Inspectors carried out a detailed inspection of the case.
- 5.5 We found several areas of non-compliance in connection with the management of the case and MI5's obligations in relation to the safety and welfare of both the CHIS and those affected by the CHIS's authorised conduct. We identified serious issues in relation to the adequacy of MI5's record keeping. In addition to these compliance issues, the Inspectors concluded, based on the material they had reviewed, that Agent X's CHIS status had been disclosed to the BBC.
- 5.6 In line with normal practice, we shared a draft copy of this report with MI5 in February 2023 to allow factual accuracy to be checked. During this process MI5 robustly asserted that, contrary to the Inspectors' conclusion, it had not departed from NCND in respect of

Agent X's CHIS status. MI5 expressed concern that the Inspectors' finding on this point, which MI5 considered to be incorrect, might have influenced the Inspectors' view of the case more generally. MI5 was invited at a meeting and, later in writing, to provide any material which supported its position, additional to the material already considered by the Inspectors.

- 5.7 In December 2023, the IPC wrote to MI5 detailing why we had reached the view that MI5 had departed from NCND and again asking MI5 to supply any contemporaneous documentary evidence which supported MI5's position. In response to the IPC's letter, MI5 provided a chronology of relevant events and several documents produced for the High Court proceedings, including the OPEN witness statement from 'Witness A' which contained an unequivocal assertion that MI5 had not deviated from its NCND policy. However, MI5 could not provide any contemporaneous material or records to support this assurance.
- 5.8 It is important to note that, from our oversight perspective, whether or not Agent X's status had been disclosed was not a material issue. Whatever had happened, there should have been an unambiguous contemporaneous record of such an important decision and any associated actions taken, and there was not. Based on MI5's assertions and its evidence provided to the High Court, we agreed to remove our finding that MI5 had departed from NCND from our inspection report. Due to the lack of contemporaneous evidence, our important findings of non-compliance regarding MI5's failure to maintain accurate records were reinforced in the final report.
- 5.9 In March 2024, the IPC wrote to the Director General of MI5 sharing a copy of the final version of the inspection report. Areas of non-compliance and observations from that report remain part of our regular inspection programme and MI5 has taken steps to improve compliance at an organisational level which we continue to monitor.
- 5.10 In late 2024, it became clear that MI5 had provided incorrect evidence to the High Court and the Investigatory Powers Tribunal (IPT), and incorrect information to IPCO. The Director General personally informed the IPC directly in mid-December 2024 and apologised to IPCO Inspectors.

Divisional Court and IPT judgments in July 2025

- 5.11 The position was also corrected in respect of the three sets of proceedings identified above. The injunction was varied by consent to allow the BBC to report on the fact that, and the circumstances in which, false evidence had been given by MI5 in the injunction proceedings. A hearing was listed before the Divisional Court to consider two issues:
 - (i) how MI5 came to provide false evidence and what further steps (if any) should be taken; and
 - (ii) whether the Attorney General and MI5 should be permitted to maintain NCND on the question of X's CHIS status.
- 5.12 However, very shortly before the hearing, MI5 confirmed that it no longer sought to maintain its NCND position, and X's status was publicly confirmed.

- 5.13 The Divisional Court handed down its judgment on 2 July 2025.³² The Court considered the conclusions of an internal investigation conducted by MI5 and an external review conducted by Sir Jonathan Jones KC (Hon.). The Lady Chief Justice summarised the Court's conclusions at paragraph 12, which included the following:

(a) The evidence that has been put before the court indicates that the special advocates, the High Court, the IPT and the Investigatory Powers Commissioner were all misled on the key question whether MI5 had departed from NCND in relation to X's CHIS status. The proper operation of each of these safeguards is dependent upon high standards of candour on the part of the agencies. Any evidence of a departure from these standards must be promptly and effectively investigated.

[...]

(d) The investigations carried out by MI5 to date suffer from serious procedural deficiencies. Their conclusions cannot presently be relied on.

(e) In those circumstances, we consider that it would be premature to reach any conclusions on whether to initiate contempt proceedings against any individual. We accordingly adjourn consideration of that question pending the outcome of a further investigation which we anticipate will not suffer from the defects that we have identified. We consider that this further investigation should be carried out under the auspices of the Investigatory Powers Commissioner, who has oversight of MI5's surveillance activities.

[...].

- 5.14 On 30 July 2025, the IPT handed down a judgment which agreed that a further investigation was required and should be undertaken under the auspices of the IPC. The President of the IPT wrote to the IPC on the same day, requesting that we undertake such an investigation and outlining several questions which should be addressed.³³

The investigation

- 5.15 Following the judgment of the Divisional Court and the request made by the President of the IPT, we began work considering the form which an investigation of the type recommended by the Court might take. A direction from the Prime Minister under section 230 of the Investigatory Powers Act 2016 (IPA) was required to extend the IPC's statutory powers to enable us formally to undertake the investigation.
- 5.16 In anticipation of the Direction and to expedite the investigation, the IPC appointed Sir John Goldring, the Deputy IPC, to lead the investigation and instructed counsel with the appropriate security clearance to support him. We set up a small team consisting of an IPCO Inspector and a project support officer, to be further assisted by IPCO senior managers and lawyers.
- 5.17 The team carried out preliminary work, including obtaining and reviewing the OPEN and CLOSED material filed with the Divisional Court and the IPT, and preparing witness lists and chronologies. The IPC wrote to Sir Ken McCallum, Director General of MI5, on a number of topics: to ensure that all documents of potential relevance to the investigation were

32 See: <https://www.bailii.org/ew/cases/EWHC/KB/2025/1669.pdf>

33 See: Letter-President-of-Investigatory-Powers-Tribunal-to-Sir-Brian-Leveson-IPC

preserved; to welcome his assurance that access to material subject to legal professional privilege would be provided on a limited waiver basis; and to seek his assurance that MI5 would provide all necessary support to ensure staff feel able to engage fully and candidly with the investigation.

- 5.18 On 15 September 2025, the IPC received a Direction from the Prime Minister. Work then began formally to gather evidence and information. Document preservation requests were sent to the Government Legal Department (GLD) and the Attorney General's Office, and detailed requests for disclosure were made to all relevant government bodies.
- 5.19 Since September 2025, numerous further requests for information have been made to relevant government bodies, individuals and the BBC. A huge volume of documents beyond those filed in the High Court and the IPT have now been reviewed by the investigation team.
- 5.20 In addition to this documentary review, 36 relevant individuals were interviewed over five weeks in November and December 2025. These included current and former staff of the intelligence services, GLD and the BBC, as well as counsel instructed on behalf of the Government in the relevant legal proceedings. As a further measure to seek to ensure that the investigation team received everything relevant, a message was disseminated to all current MI5 staff in December 2025, inviting any individuals who believe they have information which may assist to contact Sir John and his team.
- 5.21 The IPC has provided written updates to the Attorney General and the IPT throughout the investigation's work, and this will continue in 2026. All such updates are published on our website.³⁴

34 See: News – IPCO

6. Oversight activities and challenges: Northern Ireland

Overview

- 6.1 This chapter summarises the oversight activity relating to Northern Ireland which were considered during 2025. It draws together the Investigatory Powers Tribunal (IPT) litigation, the independent Angus McCullough KC review of Police Service of Northern Ireland (PSNI) practice and the steps we have taken to strengthen how cases involving confidential material are identified, recorded and brought to our attention.

McCaffrey & Birney v PSNI and others [2024] UKIP Trib 8 and associated litigation

- 6.2 On 17 December 2024, the IPT ruled on claims brought by two journalists, Barry McCaffrey and Trevor Birney, against PSNI and several other public authorities.³⁵ Matters arising from, and issues highlighted by, this litigation were a focus of our work in 2025.
- 6.3 Several of the claims considered by the IPT related to communications data (CD) acquired under previous legislative regimes. Both PSNI and the Metropolitan Police Service (MPS) conceded that they had acquired CD unlawfully in 2013 and 2012 respectively, as the 2007 “Acquisition and Disclosure of Communications Data: Code of Practice” did not provide effective safeguards where the purpose of an authorisation was to obtain disclosure of a journalistic source, and the decision-maker did not expressly consider the public interest in the protection of the confidentiality of journalistic sources.
- 6.4 One aspect of the claim related to a Directed Surveillance Authorisation (DSA) authorised by the then-Chief Constable of PSNI on 31 August 2018. The DSA sought authorisation for a week’s surveillance of an individual suspected of leaking material from the office of the Police Ombudsman of Northern Ireland to the claimant journalists. The stated objective of the surveillance was to establish whether that individual met the claimants following their arrests and the search of their offices on 31 August 2018, and to capture any conversations which took place.
- 6.5 The IPT found the DSA to be unlawful at common law and incompatible with the claimants’ Article 10 rights under the European Convention on Human Rights (ECHR), on the ground that the Chief Constable had failed to consider whether there was an overriding public interest justifying interference with the integrity of a journalistic source, and therefore failed to apply the relevant legal test.

35 See: McCaffrey and Birney Press Summary Investigatory Powers Tribunal FINAL 17 December 2024

- 6.6 This case attracted significant public attention and added to concerns regarding the use of covert investigatory powers against journalists and lawyers in Northern Ireland. In response, Chief Constable Jon Boutcher commissioned Angus McCullough KC to review PSNI's activities.³⁶
- 6.7 On 12 December 2025, the IPT handed down an interim judgment in a related case, *Kearney & BBC v PSNI and others* [2025] UKIP Trib 13,³⁷ which is ongoing. There, MI5 made a similar concession to that made by PSNI and the MPS in *McCaffrey & Birney* regarding the acquisition of CD in 2006 and 2009, under the former Regulation of Investigatory Powers Act 2000 (RIPA) regime. We will report on any significant developments arising from *Kearney* or other similar litigation in our 2026 Annual Report.

The McCullough Review

- 6.8 The McCullough Review ("the Review") examined covert surveillance of journalists, lawyers, and other individuals with "special status" by PSNI from 1 January 2011 to 1 November 2024. A comprehensive report was published in September 2025. The Review was commissioned by PSNI Chief Constable Jon Boutcher in June 2024 in response to concerns arising from the arrest of journalists Barry McCaffrey and Trevor Birney in 2018. Proceedings before the courts of Northern Ireland and the IPT held several aspects of police activity against the journalists to have been unlawful, and the case attracted significant media scrutiny.
- 6.9 The Review team, led by Angus McCullough KC, had unrestricted access to PSNI systems and records. It examined all authorisations concerning those of special status across the full range of covert investigatory powers, highlighting instances of insufficient justification or inadequate documentation. To identify these authorisations, the team identified the locations where both applications and product may be stored and developed system-specific search techniques. The Review team described this as "end-to-end" analysis.
- 6.10 The Review's methodology was necessarily very different to IPCO's: the Review's work took some 15 months, in contrast to our rolling annual inspection programme of over 600 public authorities, with inspections routinely lasting between one and three days. The Review's remit was also focused on examining all cases involving those of special status, a term not used in investigatory powers legislation, rather than providing assurance across the full range of covert investigatory powers regardless of those affected by the activity.
- 6.11 The Review made a number of recommendations. Angus McCullough KC concluded, and the IPC has agreed, that none of the Review's recommendations are inconsistent with IPCO's regulatory assessment of PSNI. Indeed, several of the Review's recommendations echo our observations at recent inspections. These include: the need for a comprehensive training plan on confidential material; an improved process for correctly recording cases involving confidential material so that they can be brought to our attention; and the importance of seeking internal legal advice in such cases. The Review observed that PSNI's complex systems made it difficult for the organisation to provide prompt and reliable disclosure: it found two examples of over-retention or non-disclosure of material in connection with the *McCaffrey & Birney* litigation. These findings reflect our repeated findings of critical non-compliance in respect of PSNI's record and product management.

36 See: The McCullough Review.pdf

37 See: <https://www.bailii.org/uk/cases/UKIPTrib/2025/13.pdf>

- 6.12 No concerns were identified by the Review in respect of targeted warrants, whether in respect of the obtaining of warrants or the handling of confidential material. Angus McCullough KC cited the double lock process and our annual inspections as important safeguards. The Review did not identify any instances of intrusive surveillance or property interference within its remit. In respect of CD, the Review considered that the post-2015 regime for CD applications seeking to identify a journalistic source was operating as it should, with the IPCO approvals system operating as “a further effective safeguard”.
- 6.13 However, several DSA and covert human intelligence source (CHIS) authorisations were identified by the Review and subject to criticism. The Review’s findings on these authorisations are set out in some detail in its report. PSNI provided us with the CLOSED Annex to the Review to assist Inspectors in identifying the relevant cases.
- 6.14 None of these authorisations had previously been brought to our attention by PSNI, despite requests to do so during each inspection. We were notified of two such cases outside the relevant inspection year, largely because of public scrutiny of the relevant cases: these were the DSA in the McCaffrey & Birney case, and a DSA in respect of the journalist Donal MacIntyre which is discussed in some detail in the McCullough Review report. Chief Constable Boutcher also wrote to the IPC on 12 September 2025, following a meeting to discuss the Review’s findings, and notified us of several further cases which PSNI had identified as potentially falling within the Review’s recommendations.
- 6.15 In December 2025, we undertook an interim inspection of PSNI, which included consideration of all the surveillance cases identified by the Review as those which should be brought to our attention and the further cases identified in Chief Constable Boutcher’s letter. We discussed PSNI’s new method of identifying cases involving confidential material to ensure that they are flagged to us in future. This system will be tested at the next scheduled PSNI inspection. Any CHIS cases referred to by the Review which fall within our inspection parameters will be considered at the next scheduled PSNI inspection. Inspectors also examined the stand-alone system used by PSNI’s Anti-Corruption Unit, and they agreed with Angus McCullough KC’s conclusion that there was no evidence of the system being used, or being capable of being used, to bypass authorisation processes.
- 6.16 In response to the Review, the IPC met with Angus McCullough KC in early 2026 to discuss his findings and any areas in which we could learn from the Review’s experiences. A further meeting will be scheduled between Angus McCullough KC and IPCO Chief Inspectors to continue these discussions. We are considering carefully whether the Review’s findings have any wider application, particularly in relation to levels of understanding, legal advice and training on confidential material across the law enforcement community.
- 6.17 After our interim inspection, we received a number of error reports from PSNI. We may report further on specific cases connected with the McCullough Review, either in the context of reported errors or IPT litigation, in subsequent Annual Reports.

The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010

- 6.18 Angus McCullough KC, in his review of PSNI’s use of covert investigatory powers against lawyers and journalists, relies on an interpretation of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010³⁸ (the

38 See: The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010

2010 Order) which differs from the IPC's interpretation. The Review's report is drafted on the basis that any surveillance taking place within court precincts falls within the 2010 Order, as any public areas of court buildings are likely to be used for the purposes of legal consultations. The IPC has to date taken a narrower view of the application of the 2010 Order, which accorded with the approach taken by the public authorities we oversee. The IPC has discussed this differing view with Angus McCullough KC. Our work on this issue is ongoing, and in 2026 we may report further on any ramifications for our oversight of PSNI or other law enforcement agencies, and any consideration of the point by the IPT.

- 6.19 The 2010 Order adopts a location-based, rather than a purpose-based, approach to the protection of legal consultations. The IPC agrees with the McCullough Review that this risks creating a 'gap' in protection for legally privileged material; however, we remain concerned that this gap extends beyond the context of surveillance on court premises. We consider that the 2010 Order should be revised to close this gap by adopting a purpose-based approach. Although this should not be used as an excuse to delay revision of the 2010 Order, wider reform may also be necessary to ensure confidential material is adequately protected under RIPA, and we will report further on this issue in our 2026 Annual Report.

7. Errors and breaches

Overview

- 7.1 Investigating errors and breaches by the public authorities we oversee is an important part of our work. The impact of errors on the rights of individuals can be grave. Accordingly, public authorities are expected to have thorough procedures in place to comply with the legislation and Codes of Practice to mitigate the risk of errors occurring.
- 7.2 We find that public authorities take errors and breaches seriously and there is a strong culture of reliable self-reporting, with public authorities informing us of the majority of errors themselves. This doctrine of self-reporting also suggests that quality assurance and oversight arrangements are sufficiently robust in most authorities to prevent errors becoming systemic.
- 7.3 We also discover potential errors during our inspections, which are then investigated by the authority concerned and formally reported to us. We scrutinise all reported matters, considering both the impact the error has had on the human rights of any individual affected and whether the report reveals any failings in the processes and safeguards in place at that authority. Our website includes details about the types of error we investigate.

Summary

- 7.4 In 2025, we received 438 error and breach reports from UK intelligence community (UKIC) and intercepting agencies. Of these, 93 did not meet the threshold for a relevant error. The remaining 345 reports, assessed as relevant Investigatory Powers Act 2016 (IPA) errors, contained 690 individual errors.³⁹ This increase is attributable to the change in the way we record interception errors at the Government Communications Headquarters (GCHQ) and a further increase in the number of interception errors from the National Crime Agency (NCA).
- 7.5 In respect to law enforcement agencies (LEAs), wider public authorities (WPAs), local authorities and prisons, there was an increase in the number of surveillance, covert human intelligence source (CHIS) and targeted equipment interference (TEI) errors (see from paragraph 7.19) and a decrease in communications data (CD) errors (see from paragraph 7.26).
- 7.6 Section 231(1) of the IPA requires the Investigatory Powers Commissioner (IPC) to inform a person of any relevant error if considered serious i.e., that it has caused them significant harm or prejudice and is in the public interest to inform them. A relevant error is defined as an error made by a public authority rather than a telecommunications operator (TO). In 2025, the IPC made determination that four errors met the serious error definition and wrote to the affected persons.

39 This includes Principles and Data Access Agreement (DAA) breaches. See: paragraph 7.9.

UK intelligence community (UKIC) errors

- 7.7 During the year, we introduced changes to the way errors were recorded, with a focus on improving efficiency and reducing administrative burden. We encouraged UKIC to report similar, low-level errors in a consolidated format where appropriate. For instance, if an internal review determined that a staff member appropriately examined bulk data but made incidental typographical mistakes such as misspelling a name or incorrectly entering a date of birth due to a mistyped digit, these issues may be collectively recorded in a single report. As a result, while the total number of individual errors has increased, the overall number of error reports remained broadly consistent with previous years.
- 7.8 We also revised the approach to recording system-related errors, particularly within the bulk interception regime. This change has resulted in an increase in the total number of errors reported by GCHQ, as individual system failures are now recorded as separate events rather than a single aggregated issue. Notwithstanding this change in methodology, overall trends in GCHQ error reporting remain consistent with previous years.
- 7.9 Other errors reported to us include those that sit outside of the IPA, such as cases where “The Principles Relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees” (The Principles) had not been correctly applied and breaches under the UK-US Data Access Agreement (DAA). We have an agreement with the relevant agencies that they record and report any breach relating to these matters in the same manner as an IPA error. Accordingly, we record and report each one as an IPA error. Table 7.1 includes this additional information as well as IPA errors.

Table 7.1: UK intelligence community (UKIC) errors, 2025

	Agency			Total
	MI5	SIS	GCHQ	
Covert human intelligence sources (CHIS)	21	3	0	24
Directed surveillance (DSA)	4	1	0	5
Property interference and intrusive surveillance (PI/IS)	6	0	0	6
Bulk personal datasets (BPD)	87	5	8	100
Bulk personal datasets: low or no reasonable expectation of privacy (7A)	0	0	0	0
Bulk personal datasets: third party (7B)	0	0	1	1
Interception ¹	39	7	18	64
Targeted equipment interference (TEI)	0	0	4	4
Bulk interception & bulk equipment interference ²	0	1	277	278
Communications data (CD)	9	0	6	15
Bulk communications data (BCD) ³	5	0	0	5
IPA Safeguards	21	7	35	63
Section 7 Intelligence Services Act 1994 (ISA)	0	0	0	0
The Principles	2	0	0	2
Data Access Agreement (DAA)	17	0	2	19
Total	211	24	351	586

Notes (applicable to tables 7.1-7.4 and figure 7.1):

¹ The GCHQ interception figure includes three interception errors by the National Technical Assistance Centre (NTAC) which is administratively part of GCHQ.

² Bulk interception and bulk equipment interference errors were previously reported under interception and equipment interference figures respectively.

³ Bulk communications data errors were previously reported under communications data errors.

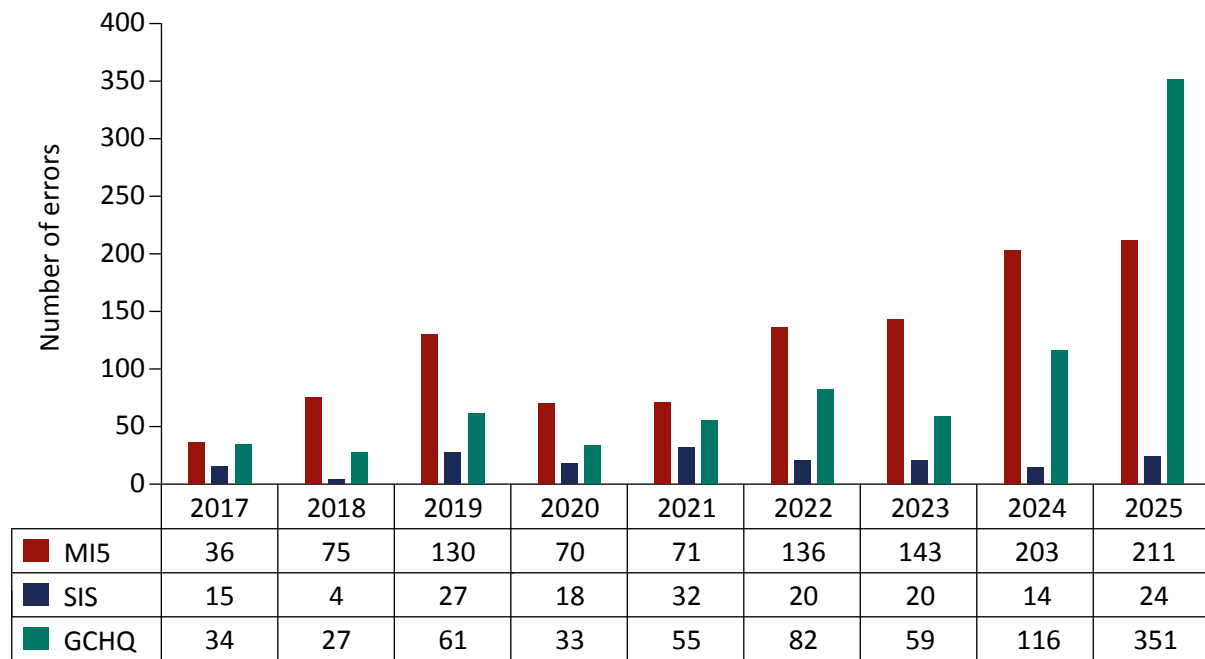
Figure 7.1: UKIC errors, 2017 to 2025

Table 7.2: MI5 errors, 2017 to 2025

	2017	2018	2019	2020	2021	2022	2023	2024	2025
Covert human intelligence sources	4	3	5	3	0	9	6	15	21
Directed surveillance	11	8	13	7	4	23	18	12	4
Property interference & intrusive surveillance	7	4	6	1	6	10	4	4	6
Bulk personal datasets	3	1	14	11	11	20	43	113	87
Bulk personal datasets: low or no reasonable expectation of privacy (7A)	-	-	-	-	-	-	-	-	0
Bulk personal datasets: third party (7B)	-	-	-	-	-	-	-	-	0
Interception	11	22	23	25	30	47	22	23	39
Equipment interference	0	0	1	2	1	6	11	4	0
Bulk interception & bulk equipment interference	-	-	-	-	-	-	0	0	0
CD (reportable)	0	37	55	14	19	20	9	9	9
Bulk CD	-	-	-	-	-	-	18	13	5
Systems	0	0	13	7	0	-	-	-	-
IPA Safeguards	-	-	-	-	-	-	1	5	21
The Principles	-	-	-	0	0	1	0	0	2
DAA breaches	-	-	-	-	-	-	11	5	17
Total	36	75	130	70	71	136	143	203	211

Notes (applicable to tables 7.2-7.4):

¹ Cells marked with “-” under The Principles, 7A, 7B, IPA Safeguards and DAA breaches indicate that these categories were introduced in the respective year and data collection began from that year onward.

² Cells marked with “-” under Systems reflect a change in methodology. From 2023, systems-related errors have been reclassified and are now reported under other relevant categories.

Table 7.3: Secret Intelligence Service (SIS) errors, 2017 to 2025

	2017	2018	2019	2020	2021	2022	2023	2024	2025
Covert human intelligence sources	10	3	9	1	6	4	0	2	3
Directed surveillance	1	0	0	1	1	0	5	0	1
Bulk personal datasets	1	0	10	6	18	13	0	6	5
Bulk personal datasets: low or no reasonable expectation of privacy (7A)	-	-	-	-	-	-	-	-	0
Bulk personal datasets: third party (7B)	-	-	-	-	-	-	-	-	0
Interception	3	1	4	8	3	0	4	3	7
Equipment interference	0	0	3	0	0	1	0	2	0
Bulk interception & bulk equipment interference	-	-	-	-	-	-	0	0	1
CD (reportable)	0	0	1	1	0	1	1	1	0
Bulk CD	-	-	-	-	-	-	0	0	0
Systems	0	0	0	0	1	-	-	-	-
IPA Safeguards	-	-	-	-	-	-	0	0	7
Section 7 ISA	0	0	0	1	1	0	9	0	0
The Principles	-	-	-	0	2	1	1	0	0
DAA breaches	-	-	-	-	-	-	0	0	0
Total	15	4	27	18	32	20	20	14	24

Table 7.4: Government Communications Headquarters (GCHQ) errors, 2017 to 2025

	2017	2018	2019	2020	2021	2022	2023	2024	2025
Covert human intelligence sources	0	0	0	0	0	1	0	0	0
Directed surveillance	0	0	3	0	0	0	0	1	0
Property interference & intrusive surveillance	0	1	1	0	0	0	1	0	0
Bulk personal datasets	0	0	1	3	0	0	0	1	8
Bulk personal datasets: low or no reasonable expectation of privacy (7A)	-	-	-	-	-	-	-	-	0
Bulk personal datasets: third party (7B)	-	-	-	-	-	-	-	-	1
Interception	32	15	51	13	30	71	7	8	18
Equipment interference	0	0	3	3	8	5	2	1	4
Bulk interception & bulk equipment interference	-	-	-	-	-	-	38	75	277
CD (reportable)	0	11	1	1	7	4	1	0	6
Bulk CD	-	-	-	-	-	-	-	5	0
Systems	0	0	0	13	9	1	-	-	-
IPA Safeguards	-	-	-	-	-	-	6	16	35
Section 7 ISA	2	0	1	0	0	0		0	0
DAA breaches	-	-	-	-	-	-	4	9	2
The Principles	-	-	-	0	1	0	0	0	0
Total	34	27	61	33	55	82	59	116	351

7.10 We received one error from the Ministry of Defence (MoD) in relation to a CHIS authorisation.

Warrant granting departments

7.11 In 2025, we received two errors from the Home Office which related to targeted interception (TI). One related to a warrant being duplicated, the second followed the Home Office sending a warrant to the wrong agency. No operational action was taken following these administrative errors.

Interception agencies

7.12 We commented in our 2024 Annual Report on an increasing trend of TI errors by the NCA, most often relating to the mishandling of intercept material, and have continued to scrutinise the situation throughout 2025. During this period, we conducted a focused interception safeguards inspection which reviewed the NCA's mitigation measures. These included the implementation of improved governance arrangements, such as a Deputy Director chaired Errors Board to improve recognition of the scale of the problem at a senior level across the agency, and a senior manager or practitioner level Error Reduction Board

to identify themes and provide ongoing advice and learning. The NCA has also revised the content and provision of specialist training and assurance mechanisms, including compliance audits. We acknowledge that the elevated level of errors is partly due to increased proactive audit activity, nevertheless the continued high level of interception errors remained a matter of concern for the IPC, who raised the matter with the Director General of the NCA during their regular meetings. We will continue to monitor the effectiveness of the training and mitigations in place to ensure its compliance with its data handling arrangements.

Table 7.5: Interception agencies errors, 2021 to 2025

	NCA	MPS	Police Scotland	PSNI	HMRC
2021	16	6	Not known	Not known	1
2022	10	3	0	1	5
2023	18	0	3	2	14
2024	47	1	2	2	4
2025	73	2	2	2	10

Note: Data for Police Scotland and PSNI for 2021 is aggregated and granular details are unavailable.

- 7.13 In addition to the figures above, there were 11 DAA breaches reported to us; eight from the NCA, two from His Majesty's Revenue and Customs (HMRC) and one from Police Scotland. The NCA also reported a breach in relation to The Principles.

Personal data breaches by telecommunications operators

- 7.14 The Investigatory Powers (Amendment) Act 2024 made provision for the reporting of personal data breaches committed by Telecommunication Operators (TO) in respect of interception, equipment interference, CD and the bulk acquisition of CD. These data breaches are now reported to us and, in relation to CD, they must be reported in parallel to the Information Commissioner's Office (ICO). The Act also provides a mechanism for the data subject to be notified where breaches are serious and it is in the public interest to do so, and to seek a remedy from the TO via the Investigatory Powers Tribunal (IPT).
- 7.15 In 2025, we reported four data breaches to the ICO relating to non-CD powers. These were investigated by the ICO and none were deemed serious breaches.
- 7.16 An example of one of these incidents, which we were made aware of by a UK TO, related to a software issue in its targeted interception system that had on three occasions between late 2024 and mid-2025, resulted in non-target traffic being routed to an intercepting agency. This traffic had been deleted after receipt since it was not required.
- 7.17 The TO was in the process of developing a replacement system. While some remedial work had been carried out which stopped the issue reoccurring, a risk remained that it could happen again before the new system was ready. We wrote to all UKIC and law enforcement intercepting agencies advising them of the issue and requesting that they make reference to this issue in all submissions for warrants, renewals and modifications where they included this TO to ensure the decision maker was fully aware.

7.18 The new system was due to be delivered in late 2025, but this timing slipped to February 2026, and then to summer 2026, with delivery expected by late 2026. We continue to monitor this situation, with support from the National Technical Assistance Centre (NTAC), and no reoccurrence of the issue has been observed.

Law enforcement agencies, prisons, wider public authorities and local authorities: surveillance, property interference, covert human intelligence sources and targeted equipment interference

7.19 Across these public authorities, the number of errors increased from 82 in 2024 to 131 in 2025. As in 2024, no errors met the statutory definition of a serious error.

Table 7.6: Total surveillance, property interference, CHIS and equipment interference errors for LEAs, wider public authorities, local authorities and prisons, 2021 to 2025

	Number of errors				
	2021	2022	2023	2024	2025
Directed surveillance	53	30	49	43	65
Property interference	15	15	24	19	19
Intrusive surveillance	0	0	3	4	2
Covert human intelligence sources (including relevant sources)	12	15	43	14	31
Targeted equipment interference	0	5	12	2	14
Total	80	65	131	82	131

7.20 Directed surveillance activity accounted for just under half of the errors reported to us. This is unsurprising given that the volume of directed surveillance authorisations granted continues to far exceed those issued for CHIS, property interference and intrusive surveillance. As in previous years, surveillance errors were predominantly due to human error, including: initiating surveillance before authorisation became effective; continuing activity after authorisation had been cancelled; or exceeding the authorised parameters, whether in tactics used or subjects being under surveillance.

7.21 In relation to CHIS, status drift remains the primary category of error. This refers to failures to identify and properly authorise the use and conduct of a source when the nature of their reporting brings them within the statutory definition of a CHIS.

7.22 While there was an increase in the number of TEI errors, these were administrative mistakes in relation to the warrant development process, for example, incorrect selection of subject matter and incomplete or missing schedules, none of which met the serious error threshold.

NCA error relating to a juvenile CHIS

7.23 Overall, only a small proportion of total errors were identified during our inspections, indicating a strong culture of self-reporting within public authorities. However, among those errors identified at inspection, particular concern arises from a series of failings by the NCA in relation to the authorisation of a juvenile CHIS. In summary:

- the NCA did not notify the IPC of the authorisation within the required seven-day period;
- the senior authorising officer (SAO) erroneously granted a 12-month authorisation, despite the statutory limit for juvenile CHIS being four months;
- the SAO failed to comply with paragraphs 4.10 and 4.15 of the CHIS Code of Practice 2022 regarding the documentation and recording of the circumstances justifying the absence of an appropriate adult; and
- incorrect authorisation dates resulted in the CHIS being tasked to engage in criminal conduct without the protection of a valid CCA.

7.24 The IPC has written to the Director General of the NCA expressing serious concern at its failure to apply appropriately a power intended for use only in exceptional circumstances and subject to stringent safeguards. The IPC has sought and received assurances that the NCA will ensure all staff involved in the management of juvenile CHIS fully understand and discharge their responsibilities.

Ministry of Housing, Communities and Local Government (MHCLG)

7.25 In our 2024 Annual Report, we reported on two errors relating to the unauthorised use of CHIS by MHCLG.⁴⁰ At our 2025 inspection we noted that MHCLG had made substantial progress towards implementing all recommended actions resulting from our review. We have subsequently confirmed with MHCLG that all actions have been completed.

Law enforcement agencies, prisons, wider public authorities and local authorities: communications data (CD) errors

7.26 The previous definitions of recordable and reportable errors were replaced in the CD Code of Practice 2025 in favour of a single category of relevant error. A relevant error occurs where both the following conditions are met:

- there has been an error by a public authority in complying with any requirements imposed by the IPA (or any other enactment) which are subject to review by the IPA; and
- CD has been acquired or disclosed wrongly.

7.27 The breakdown of errors for 2025 is shown in table 7.7.

40 Annual Report of the Investigatory Powers Commissioner 2024 (from paragraph 5.24). See: IPCO Annual Report of the Investigatory Powers Commissioner 2024

Table 7.7: Communications data errors, 2018 to 2025

	LEAs	Telecommunications operators	Postal	Other public authorities	Workflow	Total
2018	758	127	0	13	5	903
2019	755	230	0	14	12	1,011
2020	741	253	0	10	1	1,005
2021	899	332	6	15	7	1,259
2022	835	184	0	13	0	1,032
2023	1,195	346	0	10	0	1,551
2024	1,361	360	0	2	7	1,730
2025	1,280	295	0	11	52	1,591

Notes:

¹ Given the change in definition the above table includes all errors advised to IPCO as reportable errors and potential relevant errors.

² These five workflow errors related to TOs bringing the total number of TO errors to 300.

7.28 In 2025, we approved 316,961 applications for CD, and within most applications, multiple lines of CD were requested. This means the actual lines of data where an error can occur is significantly higher than the number of authorisations granted. When set against the volume of CD acquired across public authorities, the error rate remains very low.

Table 7.8: Breakdown of communications data errors by type and responsibility, 2025

	Applicant	SPoC	TO/PO
Incorrect identifier	334	262	85
Time/date	44	302	55
Data Type	0	182	32
Excess/no data	0	0	118
Other (incl. system error)	4	11	10
No IPA authority	131	21	0
Total	513	778	300

7.29 As set out in table 7.8, it remains the case that most errors are the result of human failing where there has been a simple transposition of a number or letter in a communication identifier. These errors are usually noticed before any harm or prejudice has occurred.

7.30 In 2024, revised guidance on the definitions of a TO, telecommunications services and CD led to an increase in cases where it was recognised that CD was obtained without the appropriate authority. Over time, these new providers have strengthened their internal processes, and public authorities have become more familiar with the requirements, which is reflected in an overall reduction in the number of relevant errors during this reporting period.

- 7.31 In 2025, TOs directly reported 30 CD errors to us. The remainder of TO errors (270) were brought to our attention via public authorities. Errors within TO disclosure systems have the potential to be replicated many times over. Early warning is therefore essential, and we continue to work closely with the ICO so that enforcement action can be taken if appropriate.
- 7.32 Since 2017, public authorities have been guided by the Error Reduction Strategy (ERS) to help minimise errors. The ERS, along with its updates, has been developed from our findings during investigations into serious or potentially serious mistakes. Under the 2025 CD Code of Practice, all public authorities are now legally required to follow any ERS agreed upon by the IPC and the Home Office.

Serious error investigations: CD

- 7.33 Section 231(1) of the IPA requires the IPC to notify affected individuals if a relevant error has caused significant harm or prejudice, provided it is in the public interest to do so. This notification will advise them of a right of remedy via the IPT, if one is considered available.
- 7.34 The circumstances in which we would investigate an error as potentially serious include:
- where a public authority has, as a result of a relevant error, made an arrest, searched a person's home, or made an improper disclosure of information;
 - errors that result in the wrongful disclosure of a large volume of CD or a particularly sensitive dataset; and
 - where CD has been acquired in the absence of an authorisation.
- 7.35 The 2025 Code of Practice requires reportable errors to be sent to the IPC within five to ten working days, where each report is assessed for severity. In 2025, we conducted eight serious error investigations and the summaries of these are in Annex C.
- 7.36 In three of these cases (error investigations 2, 3 and 8), the IPC found significant harm had been caused to those involved and wrote to them to notify of their rights. We identified key lessons from these cases and shared them with both the public authorities involved as well as the wider community. These learnings will also be reflected in a revised ERS in 2026.
- 7.37 In three of the TO-related cases (error investigations 4, 5 and 6), while the circumstances were grave enough to possibly warrant civil redress, we were unable to notify affected persons as the IPA only permits the IPC to notify serious errors by a public authority, not a TO. TO errors are considered through the framework of data protection legislation and are overseen by the ICO. It is challenging to identify errors in CD datasets provided by TOs without corroboration and we encourage the action demonstrated in error investigation 7, whereby six police forces collaborated to verify data inaccuracies before considering enforcement action.
- 7.38 We encourage early notification of potential errors in TO systems so relevant public authorities can be alerted. In error investigation 8, the TO issued such a warning relating to inaccuracies within a specific dataset. Unfortunately, this warning was overlooked by the public authorities involved. Public authorities are required to remain vigilant regarding notifications of potential inaccuracies in CD provided by a TO. Neglecting to address such warnings before initiating enforcement action may constitute a relevant error, and we will investigate these situations and refer them to the IPC for determination.

Serious error investigation: Prison interception

- 7.39 Section 49 of the IPA provides for the interception of communications within prison establishments if the activity is conducted in accordance with Prison Rules. One of our serious error investigations conducted during 2025 followed a complaint that a prison had intercepted calls between an inmate and their solicitor. Interception of such calls is permitted if the prison governor has reasonable cause to believe that the communication is being made with the intention of furthering a criminal purpose and authorisation is granted by the Chief Executive Officer of His Majesty's Prison and Probation Service (HMPPS).
- 7.40 Our investigation determined that the safeguards within the prison telephone system intended to prevent recording of legal communications failed in this instance. The legal telephone number was incorrectly classified as a social contact, resulting in its recording. The investigation revealed that although the calls were inadvertently recorded, the recordings were neither downloaded nor listened to and were automatically deleted after the prescribed retention period. The IPC reviewed these facts and concluded that it had an immediate effect on their calls with their solicitor in prison, which caused significant prejudice or harm to the individual. Accordingly, the person was informed of their right to seek redress.

8. Litigation in 2025

Overview

- 8.1 We have addressed legal developments and cases that have had a bearing on the work of the Investigatory Powers Commissioner (IPC) and the Investigatory Powers Commissioner's Office (IPCO) in 2025 in detail across the relevant chapters of this report.
- 8.2 These are:
- Agent X (Divisional Court and Investigatory Powers Tribunal proceedings): the judgments of the Divisional Court and the Investigatory Powers Tribunal in July 2025, and IPCO's subsequent investigation directed by the Prime Minister. [See: chapter 5].
 - Northern Ireland litigation – *McCaffrey & Birney v PSNI and others* [2024] UKIP Trib 8, and related cases: issues arising from this case, including unlawful acquisition of communications data and the treatment of journalistic material. [See: chapter 6].
- 8.3 On 7 April 2025, the Investigatory Powers Tribunal (IPT) handed down a procedural decision confirming a claim against the Home Secretary in relation to the Secretary of State's powers to make Technical Capability Notices under the Investigatory Powers Act 2016 (IPA). Although that decision falls within 2025, it was addressed in our 2024 Annual Report.⁴¹

41 Annual Report of the Investigatory Powers Commissioner 2024 (paragraphs 4.69-4.71). See: IPCO Annual Report of the Investigatory Powers Commissioner 2024

9. Protecting confidential or privileged information

Overview

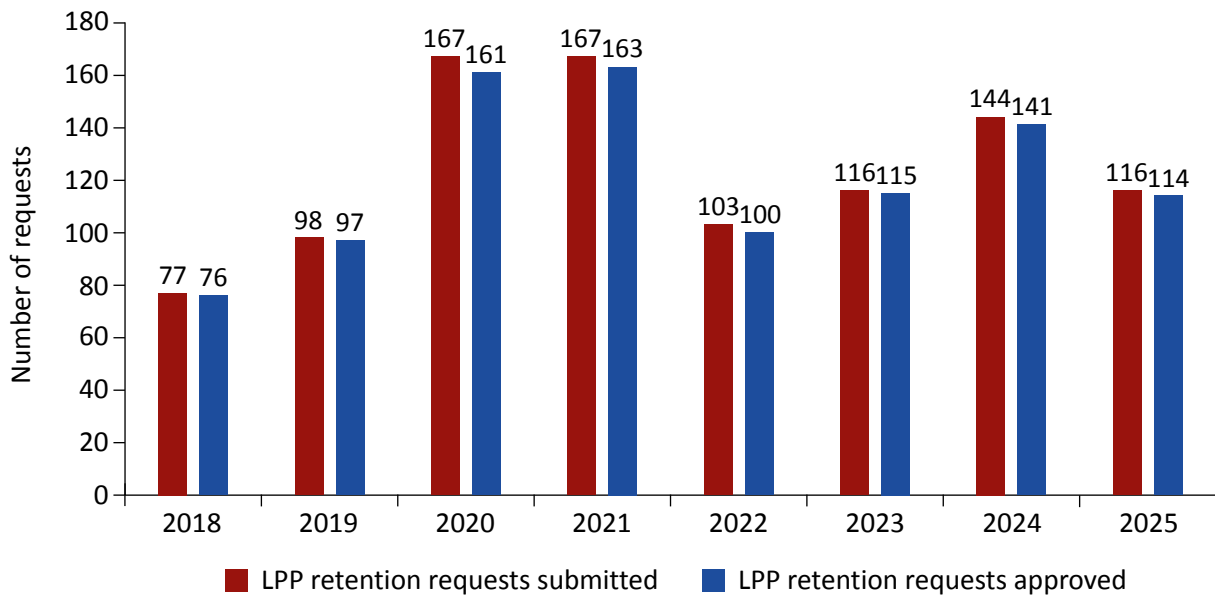
- 9.1 The Investigatory Powers Act 2016 (IPA) and its Codes of Practice provide additional safeguards for certain forms of confidential and legally privileged information. Judicial Commissioners have a statutory role in authorising and overseeing the acquisition and retention of such material. Safeguards are also set out in the Police Act 1997, the Regulation of Investigatory Powers Act 2000 (RIPA),⁴² the Covert Surveillance and Property Interference Code of Practice 2018 and the Covert Human Intelligence Sources (CHIS) Code of Practice 2022, to protect confidential and privileged information acquired from the use of such techniques without appropriate oversight.

Legal Professional Privilege (LPP)

- 9.2 Legal Professional Privilege (LPP) protects against the disclosure of confidential communications and other material attaching to such communications. It enshrines the right to seek legal advice and conduct litigation in confidence. Material subject to LPP may include conversations or written advice, which can arise between an individual or organisation and a professional legal adviser. In some circumstances, privilege may attach to confidential communications between an individual and a third party.
- 9.3 In applications, we expect consideration to be given to the likelihood of obtaining material subject to LPP. We expect consideration to be given to the public interest in protecting the confidentiality in privileged communications balanced against the public interest in obtaining the material. We would also expect to see how any material will be handled if it is obtained.
- 9.4 In the event that public authorities do obtain LPP material in their exercise of investigatory powers, they must inform us if they wish to retain that material for a purpose other than destruction. When making their decision as to retention, Judicial Commissioners will take into account the material, its proposed use and the handling conditions in order to determine whether the public interest in retaining it outweighs the public interest in the confidentiality of the material. Both public authorities and Judicial Commissioners take a stringent approach to this test.
- 9.5 In 2025, 116 applications were made in relation to the retention of LPP material. Of these, Judicial Commissioners approved 114.

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

Figure 9.1: Number of requests submitted and approved for the retention of LPP material, 2018 to 2025



Confidential journalistic material and sources of journalistic information

- 9.6 Journalistic freedom is protected under Article 10 (freedom of expression) of the European Convention on Human Rights. We would expect all relevant applications to consider the necessity and proportionality of any request in that context and demonstrate an overriding requirement in the public interest. We expect these applications to be rare.
- 9.7 Confidential journalistic material and sources of journalistic information are subject to specific safeguards, which are designed to respect the freedom of the press. All applications made under the IPA and RIPA should set out whether the purpose of the application is to obtain confidential journalistic material or identify sources of journalistic information. All applications should also state the likelihood of such material being obtained.

Communications data (CD) relating to journalists and sources of journalistic information

- 9.8 Applications relating to journalists fall into the sensitive profession category. Most applications relate to circumstances where a journalist has been a victim of crime and CD is used to identify a suspect or corroborate the evidential case. In a small number of cases the journalist is suspected of a criminal offence and CD is sought to confirm or counter the allegation. During our inspections, we scrutinise all applications and authorisations relating to journalists for compliance with the requirements set out in Chapter 8 of the 2025 CD Code of Practice.
- 9.9 Under section 77 of the IPA, authorisations for CD seeking to identify a journalistic source require the prior approval of a Judicial Commissioner. The Judicial Commissioner must be satisfied that there is an overriding requirement in the public interest to approve an application to identify a source of journalistic information.

- 9.10 In 2025, 19 applications were made under section 77. LEAs and wider public authorities made three such applications, a summary of these is set out below:

Case 1

- 9.11 A public authority applied for CD seeking to establish if a suspect had disclosed confidential financial records. Although not originally considered by the public authority to be seeking to specifically identify a source of journalistic information, as the suspect had made the disclosure to a media outlet, we treated the application as such and referred it for review by a Judicial Commissioner, after which the application was approved.

Case 2

- 9.12 This was a further application made in relation to a case reported in our 2024 Annual Report. The investigation sought to identify a person offering to sell sensitive personal data (medical records) relating to a high-profile individual to a journalistic publication. The application presented a sound intelligence case for suspecting that the information being offered had been unlawfully obtained following a breach of confidentiality and the law. The applications were approved by a Judicial Commissioner who concluded that there is a strong public interest in identifying those who breach laws designed to protect sensitive personal data.

Case 3

- 9.13 This was an investigation under section 181 of the Online Safety Act 2021, that involved a person sending a message conveying a threat of death or serious injury, intending the recipient of the message to fear that the threat will be carried out. The case concerned a message sent to a journalist threatening violence against a sporting personality and their family. The journalist worried for the safety of those involved reported the matter to the police, who made an application for CD which was approved.

Other applications relating to journalists and sources of journalistic information

- 9.14 Looking at the use of other powers, our inspections have not identified any concerns in relation to the handling of journalistic material. While there was a single occasion when an applicant should have sought a more senior authoriser for its application because of the prospect of obtaining journalistic material, no such material was in fact obtained.
- 9.15 The number of applications to acquire journalistic material in other powers will always be substantially smaller than those seeking to acquire CD (due to the relative volume of total applications) and all applications will have been subject to the double lock approval by a Judicial Commissioner. As with all authorisations, it must be necessary and proportionate to conduct the proposed interference or interception and so the test that must be satisfied here is no different. However, we expect additional consideration to be given to the confidential material that may be obtained and to the need for there to be an overriding requirement in the public interest to satisfy the threshold in this context. We would also expect applications to give some consideration to how confidential material would be handled and the extent to which such material is expected to be relevant to the investigation.

- 9.16 Under the 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 and be authorised at a more senior level. We would expect any relevant application to include details of how this sensitive material would be protected.
- 9.17 In 2025, 67 applications were made for warrants under the IPA where the purpose was to obtain material which the applicant authority believed would relate to confidential journalistic material.
- 9.18 As with CD, applications relating to sources of journalistic information must all be considered by a Judicial Commissioner (even if not relating to journalistic sources). In 2025, there were 63 warrant applications to identify a journalistic source

Additional safeguards for health records

- 9.19 The intelligence agencies may apply for a specific bulk personal dataset (BPD) warrant to retain and examine a dataset that 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. However, we can confirm that we have not identified any issues of non-compliance or made any recommendations in relation to these safeguards.

10. Technology

Overview

- 10.1 This chapter summarises technology-related developments within the Investigatory Powers Commissioner's Office (IPCO) in 2025, including enhanced inspection tools, improvements to internal systems, work to strengthen the communications data (CD) authorisations process, and our developing approach to the oversight of artificial intelligence (AI).

Remote access to records

- 10.2 We continued to expand the technology that enables Inspectors to remotely access certain law enforcement records. Building on the first use of this capability in early 2025, we conducted further remote inspections during the year. This approach offers greater flexibility and efficiency for shorter, lower-risk inspections, reducing travel demands without diminishing the rigour of our oversight. Remote access has also helped minimise disruption to public authorities and, in some cases, supported simultaneous reviews across multiple organisations, which is particularly valuable in identifying themes across work.

System improvements and operational resilience

- 10.3 In 2025, we continued to strengthen our internal systems, supported by the longer-term financial certainty provided through the Spending Review settlement. This stability enabled us to modernise key parts of our IT infrastructure, including work to streamline our warrant processes and improve the Case Management System (CMS) used for CD applications. These upgrades were essential given rising demand and the central role that the CMS plays in enabling timely and consistent decisions.
- 10.4 However, the CMS experienced two significant outages during the year, highlighting the need for continued focus on resilience and system reliability. In February, system performance degraded for just over three weeks, slowing decision-turnaround times and increasing the application queue. In December, a complete outage lasting about 34 hours led to a further increase in queue length and resulted in breaches across all Service Level Expectations (SLEs).⁴³

43 Service level expectations are:

- Priority 1 (urgent) applications: dealt with by the authorities themselves
- Priority 2: applications are to be processed within six hours
- Priority 3: applications are to be processed within 24 hours (by the end of the next working day)
- Priority 4: applications are to be processed by the end of the 6th working day

- 10.5 In response, we worked closely with the Home Office (the providers of the CMS) to address the issues identified and began a wider programme of work aimed at improving stability and strengthening its resilience. This programme also includes improvements to efficiency, quality and sustainability across the end-to-end CD authorisations process, reflecting the central importance of the CMS to our oversight functions.

Improving the CD authorisations process

- 10.6 Throughout 2025, we continued work to improve the efficiency and sustainability of the CD authorisations process. Demand for CD authorisations continues to rise, with an average annual increase of 9% between 2021 and 2025, while our resources have not grown at the same pace.
- 10.7 To manage this pressure, we progressed a programme of improvements across the end-to-end authorisations process, focusing on both internal systems and the support and guidance provided to public authorities. As part of this programme, we held engagement with key stakeholders which helped identify priorities for improvement, following which we agreed to implement several internal improvements:
- **CMS 'Error Reduction Mechanism':** A new tool that checks the decision recorded in the CMS against the written assessment. This reduces the risk of applications being approved or refused in error (for example, by selecting the wrong option) and helps save time for our staff and public authorities.
 - **Improving guidance to applicants:** We are updating our guidance to ensure all public authorities understand how to submit high-quality applications.
 - **Improving management information (MI):** Working with the Home Office, we are strengthening MI at both strategic and operational levels, including through an improved dashboard.
- 10.8 We have also worked with public authorities to introduce changes on their side. A review of applications showed that most can be completed within 1,000 words, except in more complex cases. Following a successful trial with a small number of authorities, this approach began rolling out in April 2026. We have also introduced an application "wizard", developed with the Home Office, to help applicants produce clearer and more consistent submissions, particularly where use of the power is less frequent.
- 10.9 These changes will take time to embed, particularly where technical development is needed. While no single change will resolve current pressures, together they are expected to improve efficiency and support a more sustainable process.
- 10.10 We are also exploring how AI might support faster and more efficient processing in future. While there are no immediate plans for deployment, we are working with the Technology Advisory Panel (TAP) to assess potential options and ensure our systems are ready to support these tools.
- 10.11 We thank all public authorities for their support as these changes have been introduced. We are particularly grateful to Gwent Police, Dyfed-Powys Police, the Department for Work and Pensions (DWP) and the Financial Conduct Authority (FCA), which participated in the word-limit trial. We will continue to seek feedback and will report further progress in our 2026 Annual Report.

Strengthening CD applications through NAFN collaboration

- 10.12 We worked in collaboration with the National Anti-Fraud Network (NAFN), the College of Policing and His Majesty's Revenue and Customs (HMRC), using their collective expertise to improve the quality of CD applications. This work helped strengthen understanding of the legal requirements for acquiring CD and reduced the number of applications falling below the required standard.
- 10.13 It also improved consistency in applications submitted through the NAFN platform, particularly among organisations with less experience of using these powers. By reviewing a large sample of cases, enabling us to identify good practice and share practical lessons with organisations with less experience of the process.
- 10.14 Building on this and drawing on established guidance such as the Codes of Practice and IPCO's Operational Digest, we supported the development of training materials, including workshops and webinars for the wider CD community. These have since been developed into accredited e-learning by the College of Policing and are now hosted on both NAFN and College of Policing platforms. The modules also form part of our internal induction for new staff.
- 10.15 This collaboration continues to evolve in response to changes in CD and its use, ensuring that guidance and training remain accurate, relevant and accessible.

Modernising the warrant process

- 10.16 In 2025, we continued work to develop a bespoke warrant authorisation workflow and reporting system to replace several fragmented legacy platforms.
- 10.17 Working in close collaboration with Home Office IT teams, the development follows a two-phase structure:
- Phase One covers applications at TOP SECRET and SECRET classification; and
 - Phase Two addresses applications at OFFICIAL-SENSITIVE classification.
- 10.18 We defined the required functionality and ensured continuous user input throughout the development process. Phase One went live in September 2025, delivering significant improvements for the team. Phase Two is underway, with an anticipated launch in late spring 2026.
- 10.19 The introduction of this system is expected to deliver substantial time and cost savings across this area of work. We will provide an update on this work in our 2026 Annual Report.

Artificial intelligence

- 10.20 Since mid-2024, we have been developing our approach to the oversight of AI as it relates to the Investigatory Powers Act 2016 (IPA). Early work has focused on defining what AI means for oversight and understanding how it may interact with investigatory powers, both now and in the future.

- 10.21 During 2025, we continued this work by engaging with public authorities through workshops, briefings and inspections to understand how AI may be used in practice. Using the four stages set out in our definition (Applications, Collection, Analysis and Safeguarding), we identified where AI could intersect with the use of investigatory powers and where further attention may be needed.
- 10.22 In parallel, we have continued to build the technical awareness of our staff so they can identify and assess AI-related issues during inspections. This is helping to shape our early thinking on a proportionate and sustainable approach to oversight.
- 10.23 We have also worked with international partners through the Five Eyes Intelligence Oversight and Review Council (FIORC), sharing insight and comparing approaches to AI oversight across jurisdictions.
- 10.24 In 2025, the Chair of the TAP, Professor Dame Muffy Calder, together with an IPCO official, spoke at the EOS-utvalget Conference in Norway to outline our developing approach to AI oversight.⁴⁴ This provided an opportunity to set out our thinking to an international audience and contribute to wider discussions on AI in national security contexts.
- 10.25 Our work remains at a discovery stage. We are focused on building an evidence based understanding of how AI is used by public authorities, where it may introduce new or increased risks, and how oversight can remain effective and informed. We will continue this work through 2026 and report further in our next Annual Report.

44 EOS-utvalget is Norway's parliamentary committee responsible for independent oversight of the nation's intelligence, surveillance and security services.

11. Technology Advisory Panel (TAP) Annual Report 2025

11.1 In accordance with section 246(6) of the Investigatory Powers Act 2016 (IPA), the Technology Advisory Panel's (TAP) Annual Report to the Investigatory Powers Commissioner (IPC) must be copied to the Secretary of State and Scottish Ministers. The 2025 Report was submitted in June 2026 and is reproduced below.

Foreword from Dame Muffy Calder, Chair of the TAP



*Dame Muffy Calder,
Chair of the TAP. Photo
by Ian Georgeson
Photography for the
RSE's Women in Science
in Scotland exhibition.*

It has been a privilege to chair the TAP throughout 2025. As in previous years, technological change has continued at pace, reshaping the environment in which investigatory powers are exercised. Against this backdrop, the TAP has remained focused on its role: providing clear, evidence-based advice to the Investigatory Powers Commissioner on emerging technologies and their implications for oversight.

Over the past year, Panel members have engaged with a wide range of public authorities, contributed to inspections, and supported broader discussions on how evolving technologies intersect with operational practice, including with international counterparts. This work has strengthened our understanding of both the technical landscape and the practical challenges faced by those using investigatory powers, enabling us to offer advice that is grounded in current realities.

In 2025, the Panel published its paper on AI proportionality. This work generated constructive debate across the oversight community and helped establish a clearer foundation for considering how artificial intelligence (AI) may be deployed, assessed, and safeguarded within investigatory powers frameworks. The paper reflects our ongoing commitment to ensuring that technological developments are assessed rigorously and with privacy considerations at the forefront.

I want to thank my fellow Panel members for their continued expertise and dedication, and to acknowledge the productive collaboration we have had with IPCO officials, Judicial Commissioners and external stakeholders. I would also like to acknowledge the significant contributions of Karen Danesi and Daryl Burns, who departed the Panel at the end of 2025. As we look ahead, the TAP will continue to support IPCO in ensuring that technological advancements are understood, scrutinised, and reflected appropriately in the oversight of investigatory powers.

A handwritten signature in dark ink that reads "M Calder". The signature is written in a cursive, flowing style.

Professor Dame Muffy Calder, FRSE FREng, Chair of the Technology Advisory Panel

Remit of the TAP

- 11.2 The TAP was established under sections 246-247 of the IPA. Establishing and maintaining the TAP is the responsibility of the IPC, although the Panel may also provide advice to relevant Ministers. The TAP has a dual statutory function:
- to advise on the impact of changing technology; and
 - to advise on the availability and development of techniques to use investigatory powers while minimising interference with privacy.
- 11.3 This remit ensures that the Panel provides independent, technically informed insight into how investigatory powers are exercised in a rapidly evolving technological environment.

Membership of the TAP

- 11.4 The TAP comprises experts with backgrounds in academia, government, and industry, ensuring a breadth of knowledge. Since 1 March 2022, Dame Muffy Calder has chaired the TAP. Biographies of all TAP members can be found on the IPCO website, and TAP members during 2025 included:⁴⁵
- Daryl Burns (served until the end of 2025);
 - John Davies;
 - Karen Danesi (served until the end of 2025);
 - Professor Richard Mortier; and
 - Professor Dame Alison Etheridge
- 11.5 This multidisciplinary composition enables the TAP to provide balanced and technically robust advice across the full spectrum of investigatory powers.

Key achievements in 2025

- 11.6 The TAP's work during 2025 focused on supporting IPCO's oversight role through clear, practical and forward-looking advice on emerging technologies.

AI Proportionality Paper

- 11.7 The Panel completed and published its paper on AI proportionality, which examined how AI may be used in investigatory contexts and how proportionality assessments should take account of automation, model behaviour, and uncertainty. The publication generated significant interest among public authorities, technical audiences and civil society, and supported wider discussions across the oversight community.⁴⁶

⁴⁵ See: Technology Advisory Panel – IPCO

⁴⁶ See: AI-Assessment-Framework.pdf

Support to inspections

- 11.8 Panel members contributed to several inspections across public authorities, helping to assess how new technologies are being adopted and how they affect operational workflows, privacy safeguards and compliance. These contributions enhanced IPCO's understanding of the technical dimensions relevant to the use of investigatory powers.
- 11.9 TAP members participated in several inspections over the year, including at:
- MI5;
 - Secret Intelligence Service (SIS);
 - Government Communications Headquarters (GCHQ);
 - Metropolitan Police Service (MPS); and
 - the National Crime Agency (NCA)

Advisory input across IPCO

- 11.10 Throughout the year, the TAP provided advice to the Judicial Commissioners and IPCO teams on topics including encryption, data-processing techniques, new communications technologies and emerging industry capabilities. This advice supported both authorisation decisions and broader oversight activity.

Engagement and knowledge-sharing

- 11.11 The TAP engaged with industry specialists, academic researchers and operational practitioners to deepen its understanding of developments in technology and their implications for investigatory powers. These discussions ensured the Panel's advice remained timely, relevant and grounded in the latest technical evidence.
- 11.12 The TAP also engaged on an international basis with Dame Muffy Calder, along with an IPCO official, speaking at the EOS-utvalget conference in Norway.⁴⁷ Dame Muffy Calder covered the theoretical foundations of AI as relevant to oversight, providing the conceptual and technical frame to the wider discussion on AI.
- 11.13 In November 2025, Dame Muffy Calder and Karen Danesi contributed to a Five Eyes Intelligence Oversight and Review Council (FIORC) panel session on the UK's TAP. The session set out the Panel's remit and ways of working under the IPA, gave an overview of the AI Proportionality Assessment Aid and discussed how AI could change the investigatory powers landscape and the oversight questions this may raise.

47 EOS-utvalget is Norway's parliamentary committee responsible for independent oversight of the nation's intelligence, surveillance and security services.

12. Statistics

Overview

- 12.1 Each year, we compile data on the use of investigatory powers. With the changes we implemented in 2020 to improve our data collection process now fully embedded, our current focus is on using these refined methods to ensure the effective collection of data. Our goal is to gather the necessary data in a manner that is both precise and proportionate.
- 12.2 We are mandated to provide statistics on investigatory powers by section 234 of the Investigatory Powers Act 2016 (IPA). While we adhere to these statutory requirements, we also strive for maximum transparency without compromising national security or unduly impeding the operational effectiveness of those we oversee. We try to avoid presenting statistics that could be partial or misleading. Consequently, our statistical publications may be limited in scope in areas where detailed contextual information, particularly concerning the activities of intelligence agencies, cannot be made public.
- 12.3 We believe the statistics we have chosen to publish accurately reflect the use of investigatory powers and the extent of authority exercised. We invite feedback on the relevance of the statistics presented and the transparency of our reporting.⁴⁸

Warrants and authorisations

- 12.4 In 2025, 366,976 warrants and authorisations were issued across all powers. Table 12.1 provides a further breakdown of this number. Law enforcement agencies (LEAs) continue to account for the highest proportion of authorisations due to their significant use of communications data (CD) powers.

⁴⁸ Reference to statistics from the UK intelligence community (UKIC) refer to the Security Service (MI5), the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) plus the Ministry of Defence (MoD). NB: some powers are only available to the three agencies.

Table 12.1: Investigative and other powers authorised by public authority sector, 2020 to 2025

	UKIC	LEA	WPA	Local authorities	Prison services	Total
2020	18,119	251,674	1,130	588	181	271,692
2021	17,458	284,815	870	368	271	303,782
2022	17,693	298,800	1,461	425	332	318,711
2023	14,892	319,562	2,371	518	272	337,615
2024	17,330	342,864	2,567	631	264	363,656
2025	19,635	343,230	3,098	768	245	366,976

Notes:

Figures from public authorities (collected through an external statistical questionnaire) include all CD authorisations, including those not submitted to IPCO. These may be authorised under alternative sections of the IPA (e.g., national security under section 61) and are therefore not directly comparable with IPCO's internal figures.

- 12.5 Table 12.2 sets out the total number of warrants and authorisations issued, considered and approved in 2025. This table also includes details on specific notifications to the Investigatory Powers Commissioner's Office (IPCO), as well as the total number of submissions that were refused by Judicial Commissioners. In 2025, a total of 30 applications were refused.
- 12.6 Judicial Commissioners also have the option to request further information on an application before making a decision. There may also be internal discussion with our Legal Team, Inspectorate and Technology Advisory Panel (TAP). In 2025, there were 117 cases where Judicial Commissioners sought external clarification and for most of these, sufficient information was provided, or the application was revised by the applicant to enable it to be approved.⁴⁹

⁴⁹ To note, this figure excludes communications data applications returned for rework.

Table 12.2: Breakdown of authorisations, notifications and refusals, including those considered by a Judicial Commissioner, 2025

	Considered by a Judicial Commissioner	Approved, issued or given	Refused by a Judicial Commissioner
Regulation of Investigatory Powers Act 2000 (RIPA)			
CHIS including juveniles and relevant sources	–	2,314	–
CHIS and relevant source criminal conduct authorisations	821	821	n/a
Relevant source notifications ¹	–	1,279	–
Directed surveillance	n/a	7,170	n/a
Intrusive surveillance	–	591	–
Investigatory Powers Act 2016 (IPA)			
Bulk personal datasets – class warrant	58	58	0
Bulk personal datasets – specific warrant	48	48	0
Bulk personal datasets – Part 7A category authorisations	4	4	0
Bulk personal datasets – Part 7B	38	34	4
Directions under section 219	0	0	0
Directions under section 225	0	0	0
Bulk communications data acquisition warrant	16	16	0
Communications data authorisation	n/a	346,998	n/a
Requests to identify journalistic sources using communications data under section 77	19	19	0
Bulk interception warrant	25	25	0
Targeted examination of interception warrant	102	102	0
Targeted interception warrant	3,531	3,524	7
Bulk equipment interference warrant	37	37	0
Targeted examination of equipment interference warrant	103	103	0
Targeted equipment interference warrant	3,488	3,471	17
Mutual assistance warrant	0	0	0
Request to retain legal professional privileged material ²	116	114	2
Other			
Property interference under Section 5 of the Intelligence Services Act 1994	n/a	565	n/a
Property interference under the Police Act 1997	–	1,029	–

Notes:

¹ These notifications relate to a new undercover operative deployment and an operative may be deployed on multiple operations.

² Figures from public authorities (collected through an external statistical questionnaire) include all CD authorisations, including those not submitted to IPCO. These may be authorised under alternative sections of the IPA (e.g., national security under section 61) and are therefore not directly comparable with IPCO's internal figures.

Statutory purpose of applications

12.7 Table 12.3 provides the total number of authorisations by statutory purpose across the different investigatory powers. It is worth noting that a single application could employ more than one statutory purpose.

Table 12.3: Authorisations by statutory purpose, 2021 to 2025

	Prevent/ detect crime	Preventing death or injury	National security	Identify person	Interests of public safety	Economic well-being	Other
2021	268,697	36,663	13,772	814	418	360	142
2022	256,091	47,853	16,374	979	537	223	116
2023	326,080	60,134	13,276	1,051	839	292	67
2024	278,598	54,303	13,803	980	575	512	57
2025	288,329	68,744	16,770	909	956	714	110

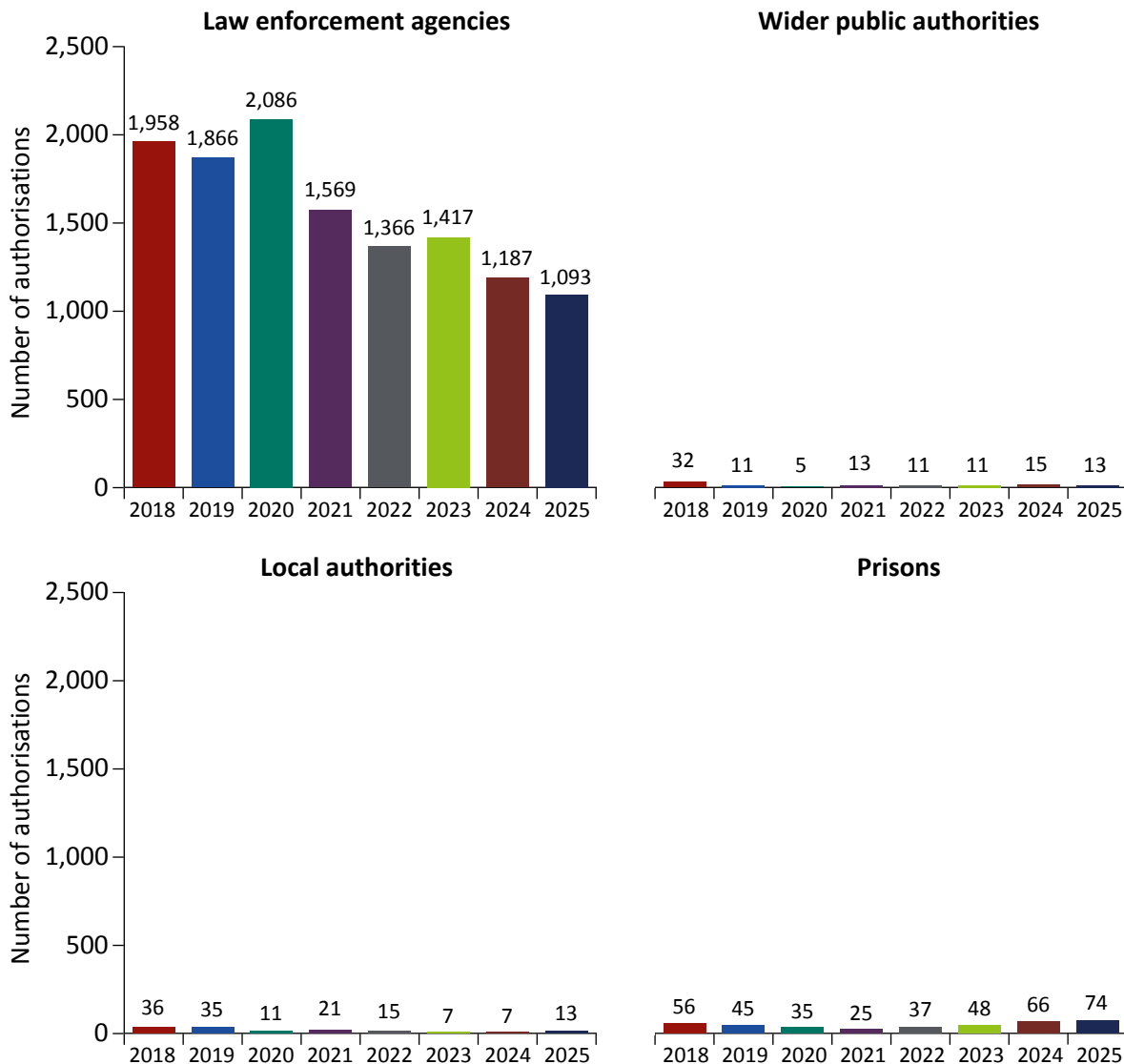
Notes:

The breakdowns by statutory purpose and crime type are derived solely from external returns and are subject to variation in how public authorities categorise authorisations. These figures may not align with total volumes or internal reporting.

Covert human intelligence sources (CHIS)

12.8 Figure 12.1 shows the total number of covert human intelligence source (CHIS) authorisations made in 2025 across LEAs, wider public authorities (WPAs), local authorities and prisons. In total, 1,193 authorisations were made in 2025 across these sectors. Of the 1,093 authorisations to LEAs, five of these were urgent.

Figure 12.1: Covert human intelligence sources across law enforcement agencies, wider public authorities, local authorities and prisons, 2018 to 2025



Juvenile CHIS

- 12.9 Of the 1,193 CHIS authorisations granted, only one related to a juvenile. The individual was not under the age of 16 at the time the authorisation was granted.

Criminal Conduct Authorisations

- 12.10 The Covert Human Intelligence Sources (Criminal Conduct) Act 2021 amended the Regulation of Investigatory Powers Act 2000 (RIPA) providing a statutory route to obtain criminal conduct authorisations (CCAs) from August 2021. In 2025, Judicial Commissioners were notified of 838 individuals authorised under this legislation. The number of CHIS or relevant source CCAs made under section 29B of RIPA where a CCA was obtained totalled 821. It is worth noting that a single authorisation for criminal conduct may involve multiple people and a single operative might be authorised on a number of operations throughout the year. Table 12.4 sets out the authorisations made since 2022.

Table 12.4: CHIS and relevant source Criminal Conduct Authorisations (CCAs), 2022 to 2025

	Total
2022	559
2023	691
2024	739
2025	821

Relevant sources

12.11 Renewals for authorisations for relevant sources (or LEA undercover police operatives) must be approved by a Judicial Commissioner at the 12-month stage. Table 12.5 sets out the number of relevant source applications and authorisations since 2020.

Table 12.5: Relevant sources authorisations and applications, 2020 to 2025

	Total Applications (incl. renewals) ²	Total Authorisations (incl. renewals)	Urgent	Renewals (long term authorisations)	Judicial Commissioner refusals ³
2020	301	293	2	75	0
2021	495	434	4	74	0
2022	526	433	1	103	0
2023	642	545	0	128	0
2024	549	465	4	102	0
2025	607	492	3	102	0

Notes:

¹ Prior to 2020, we reported data on “notifications” and cancellations of relevant sources. We no longer collect or report this data from public authorities.

² Applications include notifications to IPCO of authorisations and applications to renew authorisations after 12 months.

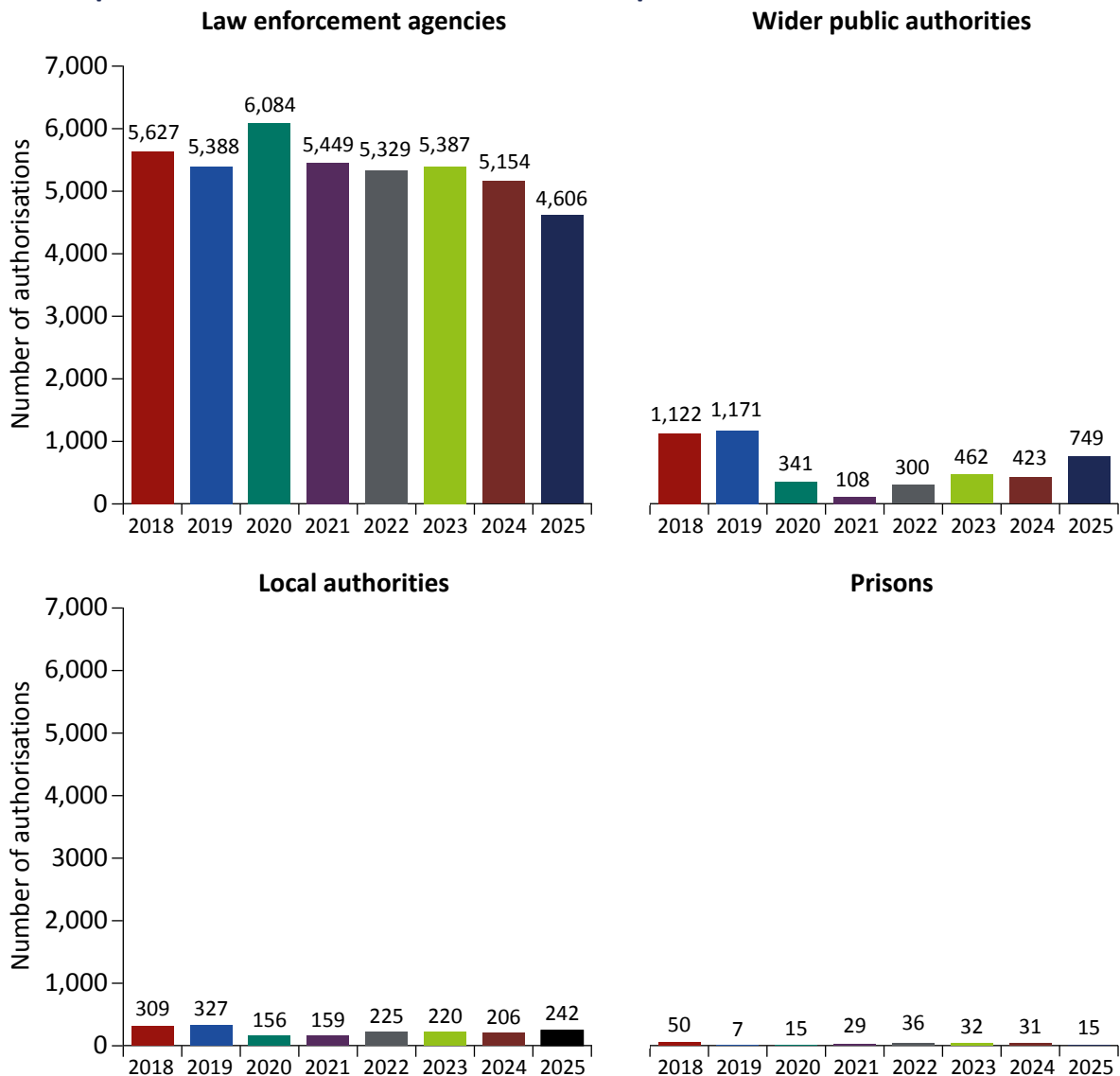
³ Refusals relate to applications to renew only.

Directed surveillance

12.12 Figure 12.2 shows that a total of 5,612 directed surveillance authorisations were made in 2025 across LEAs, WPAs, local authorities and prisons. Of these authorisations, 459 were made under urgent provisions.

12.13 In 2025, 24 applications were granted where information attracting legal professional privilege (LPP) was either sought or likely to be obtained. A further 22 applications were granted which either sought or were likely to obtain confidential material (other than LPP).

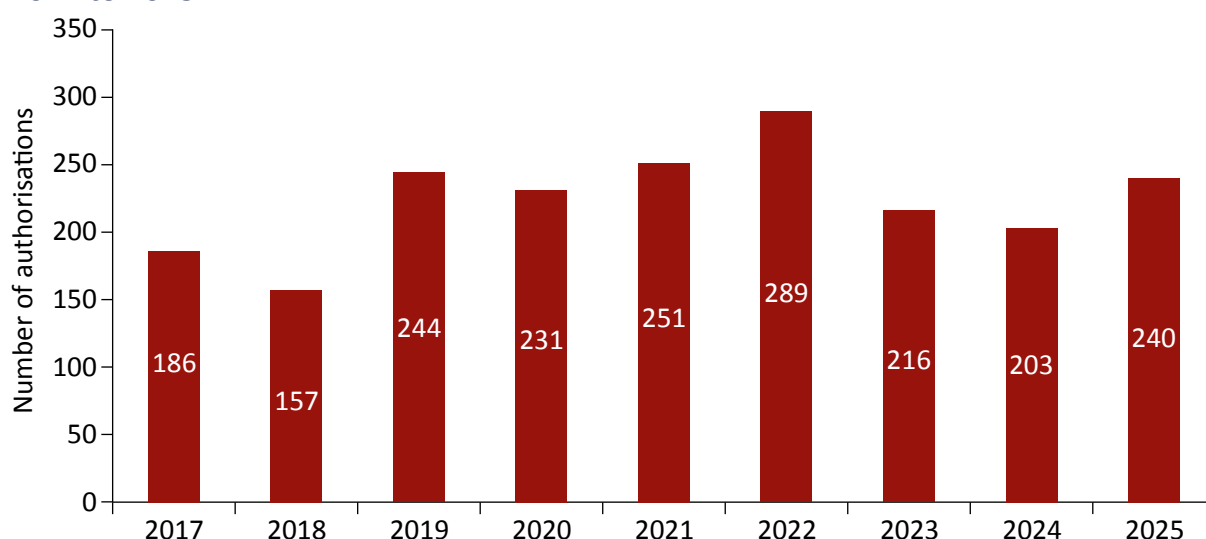
Figure 12.2: Directed surveillance authorisations across law enforcement agencies, wider public authorities, local authorities and prisons, 2018 to 2025



Intrusive surveillance

- 12.14 In 2025, 240 authorisations were granted to LEAs. Of these, 14 were urgent authorisations and two authorisations either sought or were likely to obtain confidential or privileged material which was other than LPP. A further 12 were granted where information attracting LPP was either sought or likely to be obtained.

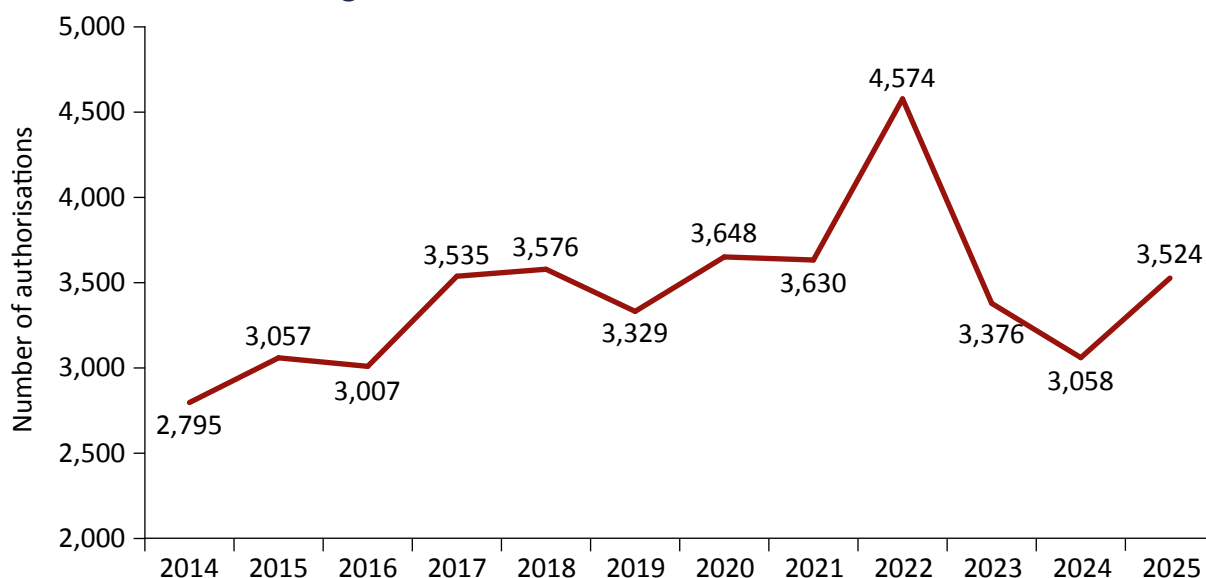
Figure 12.3: Intrusive surveillance authorisations for law enforcement agencies, 2017 to 2025



Targeted interception (TI)

12.15 Figure 12.4 shows the number of targeted interception (TI) warrants authorised in 2025. A total of 3,524 authorisations were made, of which 252 were urgent.

Figure 12.4: Targeted interception authorisations for the UK intelligence community and law enforcement agencies, 2014 to 2025



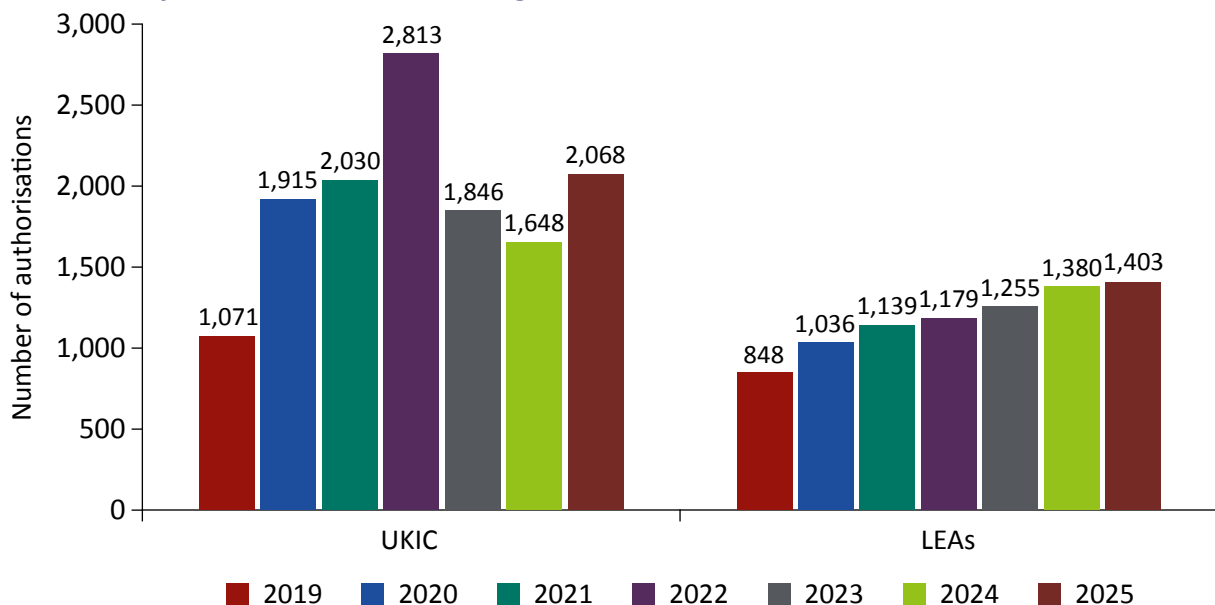
12.16 Table 12.6 sets out the number of TI warrants granted that involved either deliberate attempts to obtain legally privileged material (LPP – sought) as part of the purpose of the intercept warrant, warrants where it was likely or possible that LPP would be obtained (LPP – possible) or warrants relating to sensitive professions. As set out in the 2025 Code of Practice, all warrants that involve such confidential material are subject to additional scrutiny at inspection. The material produced by such warrants is also subject to additional safeguards in accordance with the 2025 Code of Practice.

Table 12.6: Targeted interception warrants involving confidential material, 2020 to 2025

	LPP – sought	LPP – possible	Sensitive professions
2020	12	359	35
2021	11	187	11
2022	29	211	59
2023	14	313	88
2024	11	436	88
2025	15	215	85

Targeted equipment interference (TEI)

12.17 In 2025, 3,471 authorisations were granted to use targeted equipment interference (TEI) powers, of which 569 were urgent. As was the case over the past five years, the three WPAs with access to TEI powers made no use of them in 2025.

Figure 12.5: Targeted equipment interference authorisations for the UK intelligence community and law enforcement agencies, 2019 to 2025

12.18 Table 12.7 shows that confidential material was only sought or likely to be obtained in a small number of TEI warrants.

Table 12.7: Targeted equipment interference warrants involving confidential material, 2020 to 2025

	LPP – sought	LPP – possible	Sensitive professions
2020	14	207	66
2021	15	64	14
2022	29	499	63
2023	12	213	88
2024	17	339	83
2025	19	82	66

Communications data

12.19 In total, 346,998 CD authorisations of all kinds were made in 2025. These included applications made under section 60A, as authorised through IPCO; warrants authorised under section 61 in the interests of national security (which were not authorised through IPCO); and those made under the urgent provisions. Table 12.8 shows the totals by sector and, as was the case in previous years, LEAs remain the greatest users of the power, responsible for over 330,000 of all authorisations made.

Table 12.8 Communications data authorisations, 2020 to 2025

	UKIC	LEA	WPA	Local authorities	Prison services	Total
2020	11,444	239,086	969	212	155	251,866
2021	10,531	273,193	749	237	217	284,927
2022	9,200	287,374	1,150	258	259	298,241
2023	8,458	308,239	1,898	291	192	319,078
2024	10,820	332,033	2,129	418	167	345,567
2025	11,750	332,245	2,335	513	155	346,998

Notes:

Figures from public authorities (collected through an external statistical questionnaire) include all CD authorisations, including those not submitted to IPCO. These may be authorised under alternative sections of the IPA (e.g., national security under section 61) and are therefore not directly comparable with IPCO's internal figures.

12.20 CD applications are used to request one or more data items. In 2025, in excess of 1.5 million data items were obtained, broadly similar to 2024, noting that the figures are subject to a margin of error given the volume of requests.⁵⁰

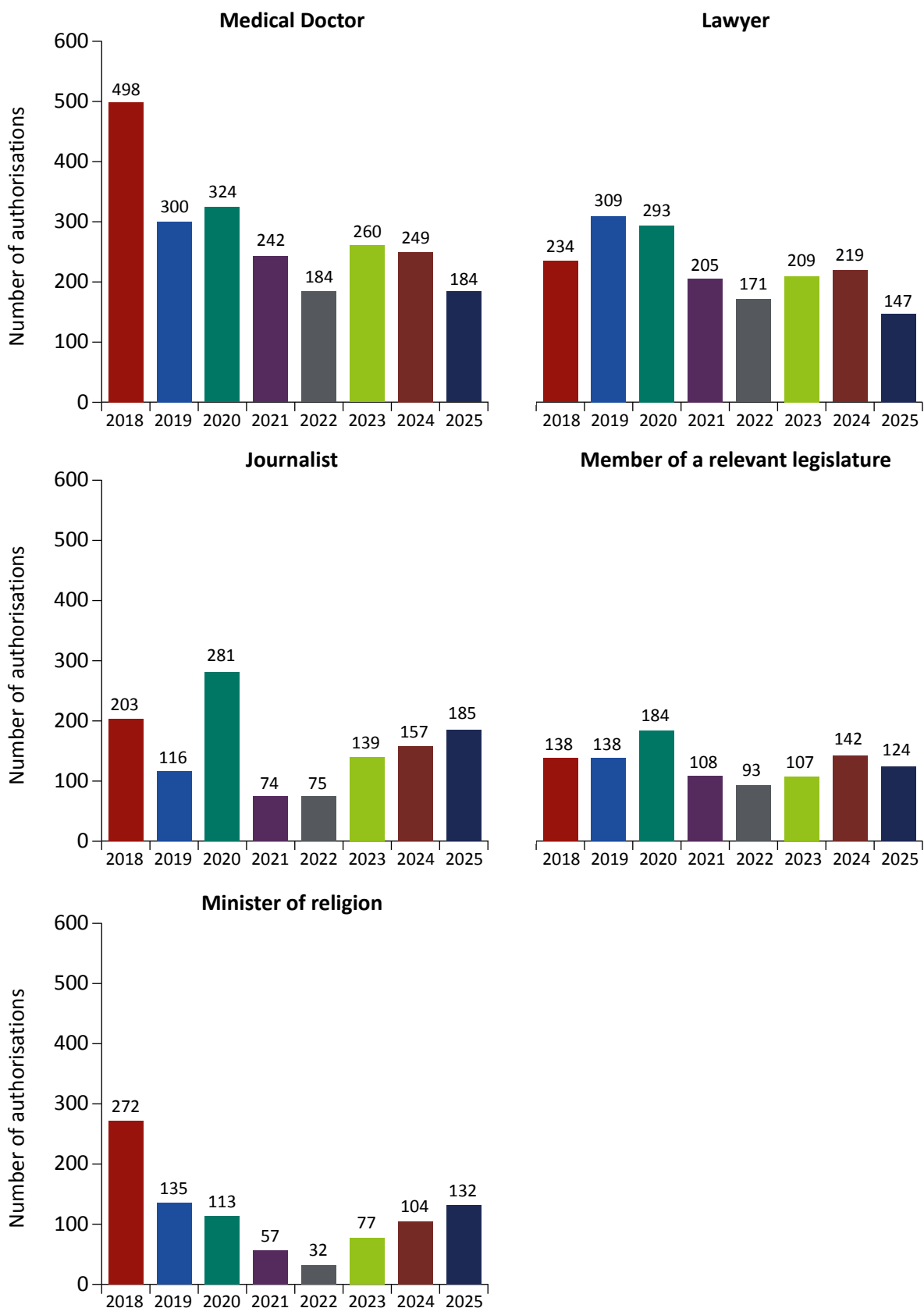
12.21 Figure 12.6 sets out the number of authorisations obtained in relation to sensitive professions. With the exception of relevant subscriber data, CD acquired and disclosed under the IPA does not include the content of communications. Nonetheless, it must be considered whether there is a risk that acquiring the data could create an unjustified risk that sensitive professional contacts will be revealed, or that there could be other substantive adverse consequences against the public interest. The 2025 CD Code of

50 This figure excludes UKIC authorisations.

Practice (from paragraph 8.8) requires applicants to give special consideration to requests for CD that relate to persons who are members of professions which handle privileged or otherwise confidential information. This can include, for example, lawyers, journalists, members of relevant legislatures, ministers of religion or doctors.

- 12.22 Public authorities must record the number of such applications and report to the IPC annually. Most applications relating to sensitive professionals were submitted because the individual had been a victim of crime. For example, it might be the case that a Member of Parliament or a lawyer received threatening or malicious calls, and CD requests were made to attribute phone numbers or email addresses to perpetrators.

Figure 12.6: Communications data authorisations involving members of a sensitive profession, 2018 to 2025



- 12.23 A total of 19 applications for CD were made to confirm or identify a journalist's source, two of which were urgent. There were no Judicial Commissioner refusals in relation to these applications. A further 63 applications were made across all powers to identify journalists' sources.
- 12.24 Table 12.9 shows the number of CD authorisations for each of the seven statutory purposes. Prevention and detection of crime remains the principal purpose, representing 76.5% of the total authorisations.

Table 12.9: Communications data authorisations by statutory purpose, 2020 to 2025

	Prevention and detection of crime	Preventing death or injury	National security	Identify person	Public safety	Economic well-being	Investigations into alleged miscarriages of justice
2020	263,383	31,257	11,470	581	221	60	4
2021	257,338	36,663	10,425	814	246	45	6
2022	242,460	47,853	9,011	979	474	14	8
2023	314,229	60,140	8,824	1,051	804	60	34
2024	267,162	54,303	10,734	980	529	74	8
2025	275,429	68,744	14,009	909	909	69	20

Notes:

The breakdowns by statutory purpose and crime type are derived solely from external returns and are subject to variation in how public authorities categorise authorisations. These figures may not align with total volumes or internal reporting.

- 12.25 For each CD authorisation where the statutory purpose is "prevention and detection of crime", public authorities which can use this purpose are required to keep a record of what types of crime the authorisation relates to. A single authorisation may relate to more than one of the crime categories (as shown in detail in table 12.10), which is why the total number of crime types exceeds the number of authorisations shown in table 12.5 above.
- 12.26 Table 12.10 shows the number of authorisations where CD is being sought for an "applicable" crime as set out in section 60A(7), 61(7) or 61A(7) of the IPA. Drug offences make up the largest number of authorisations (28.5%), followed by violence against the person (14.6%) and sexual offences (13.6%).

Table 12.10: Communications data authorisations by crime type under the “prevent and detect crime” statutory purpose, 2020 to 2025

	2020	2021	2022	2023	2024	2025
Violence against the person	26,443	23,371	28,463	46,827	37,364	51,842
Violence against the person – homicide	14,392	13,976	14,561	18,570	12,628	11,086
Theft offences	5,950	4,947	7,491	7,242	9,197	7,931
Terrorism offences	2,048	2,050	1,649	2,055	1,368	1,118
Sexual offences	30,815	34,800	39,524	46,983	55,741	48,305
Robbery offences	6,917	5,277	8,375	12,262	11,414	8,430
Public order offences	2,977	3,058	2,462	2,988	2,757	1,720
Possession of weapons offences	13,336	12,154	6,993	20,049	14,507	8,537
Other	37,343	27,572	13,341	21,303	21,075	45,743
Miscellaneous crimes against society	9,153	11,128	18,636	17,359	13,714	14,343
Harassment	7,056	9,435	9,762	13,738	12,929	14,614
Fraud and Deception Offences	15,955	20,392	19,968	24,105	26,829	22,572
Drugs Offences	81,861	87,277	125,494	146,191	114,527	100,700
Criminal Damage	551	666	636	662	1,094	1,003
Burglary	11,513	11,183	13,333	19,586	14,942	14,920
Arson	1,447	1,052	1,249	1,606	1,125	1,027
Total	267,757	268,338	311,937	401,526	351,211	353,891

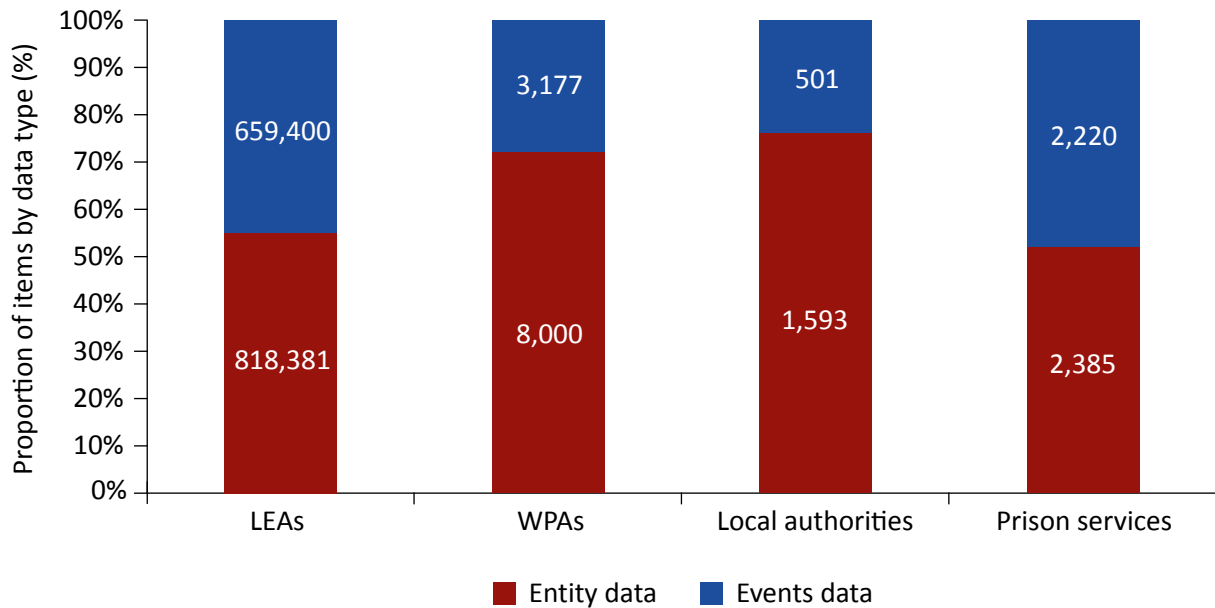
Notes:

The breakdowns by statutory purpose and crime type are derived solely from external returns and are subject to variation in how public authorities categorise authorisations. These figures may not align with total volumes or internal reporting.

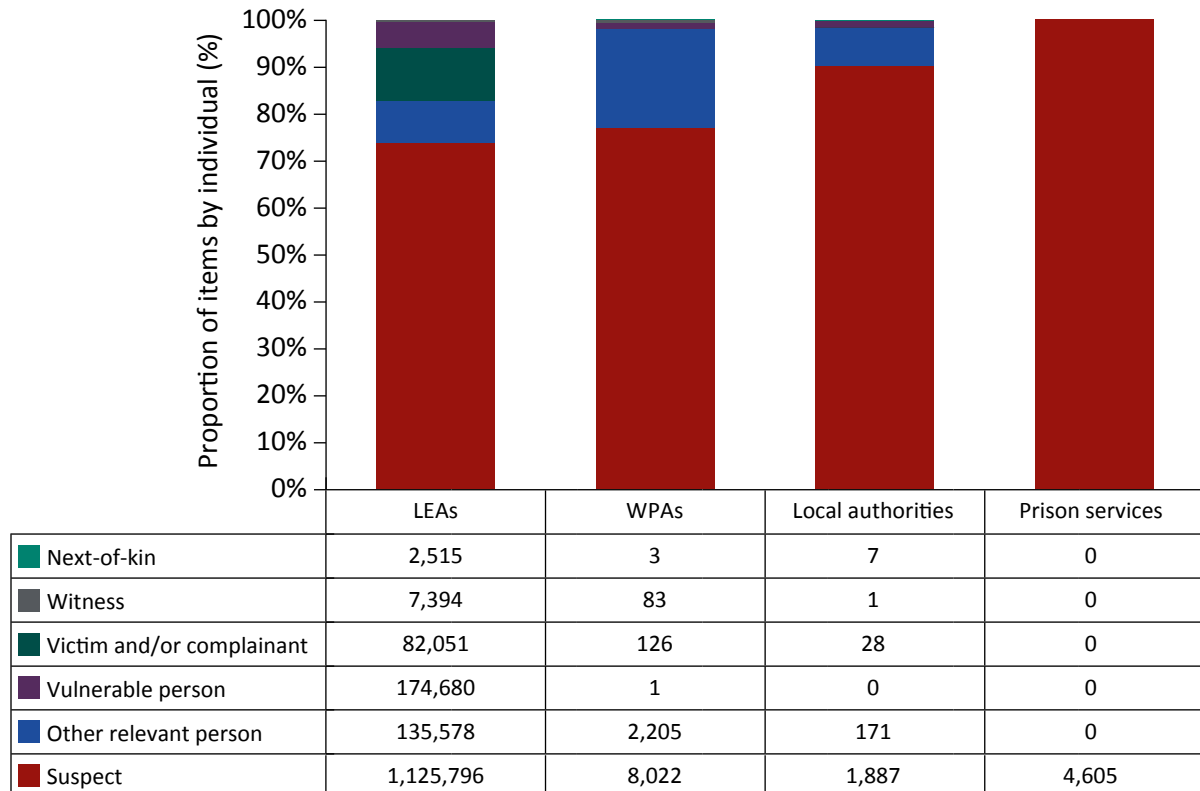
12.27 Figure 12.7 shows the total number of CD items sought in authorised applications by whether the items of data were categorised as either events or entity data.⁵¹

51 All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories:

- entity data: this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices); and
- events data: events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

Figure 12.7: Communications data items by data type, 2025

12.28 Figure 12.8 sets out the number of items of CD sought categorised by the subjects of the authorisations. One authorisation may relate to more than one category of subject.

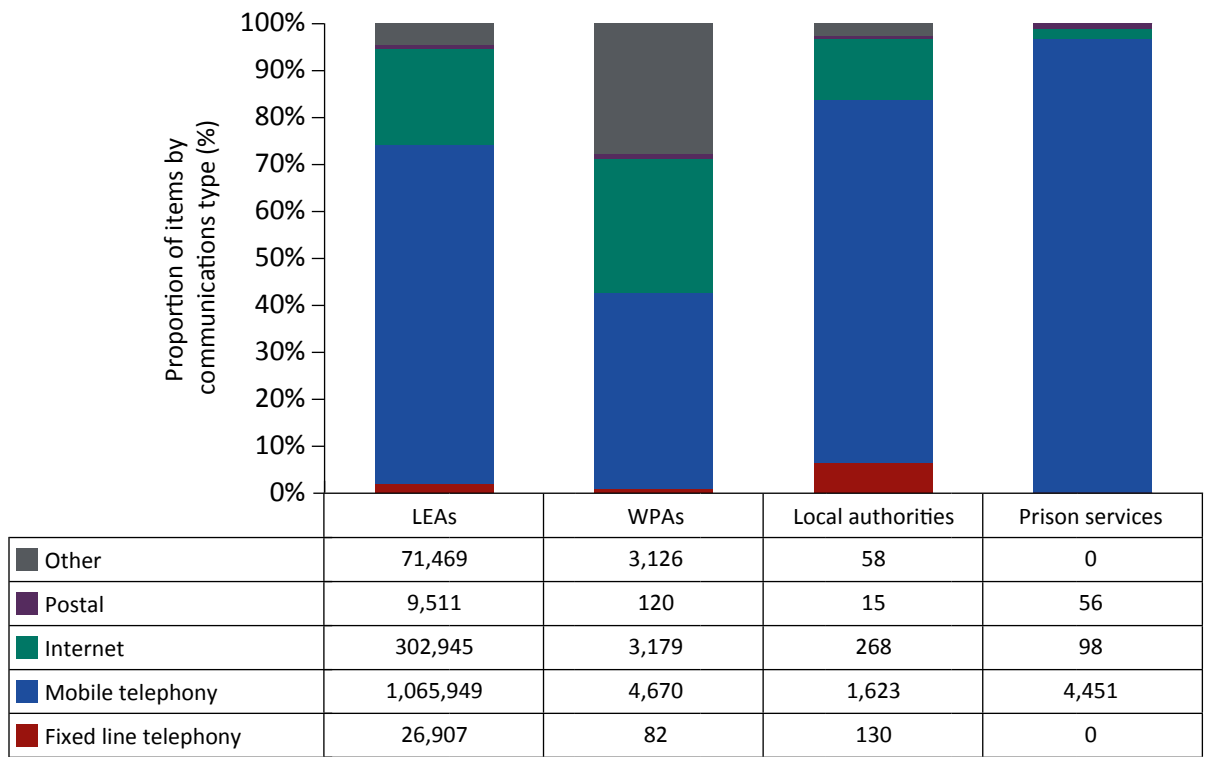
Figure 12.8: Communications data items by individual (subject), 2025

Notes:

Other relevant person refers to individuals connected to an investigation who do not fall within the standard subject categories (such as suspect, victim, or witness).

12.29 Figure 12.9 shows the total number of items of CD sought by the types of data that is being sought. An authorisation may involve several different data types and multiple items. It should be noted that, just because the items of CD were sought, it does not mean they were subsequently obtained.

Figure 12.9: Communications data items by communications type, 2025



Applications submitted to IPCO

- 12.30 In 2025, we received 349,097 CD applications, excluding those which were withdrawn by authorities, as shown in table 12.11 and 12.12.
- 12.31 In the six years since 2020 the volume of CD applications submitted to IPCO has increased each year. The largest percentage increase of 11.49% happened between 2022 and 2023, and the percentage increases have reduced each year since then. The percentage increase between 2024 and 2025 was 8.7% which reflected an increase of 28,028 applications.
- 12.32 It is important to note that these internal statistics differ from externally reported figures. Internal data is centrally managed and subject to robust quality assurance, providing a reliable and consistent basis for assessing long-term trends. In contrast, external data is collected from a wide range of public authorities and is more susceptible to variation in recording practices, definitions and data quality.

Table 12.11: Volumes of applications submitted to IPCO, 2020 to 2025

	Total applications	Year-on-year change	Year-on-year change (%)
2020	226,383	-	-
2021	245,272	18,889	8.3%
2022	270,842	25,570	10.4%
2023	301,957	31,115	11.5%
2024	321,069	19,112	6.3%
2025	349,097	28,028	8.7%

Notes:

¹ These figures are derived from IPCO's internal systems and reflect applications submitted directly to IPCO. They are subject to robust validation and quality assurance processes. These data are considered reliable and consistent across reporting periods.

² In contrast, external statistics are collected from a wide range of public authorities, each with varying recording practices and data quality controls. These differences can lead to discrepancies between the two datasets, particularly in total volumes, statutory purpose classifications and crime type breakdowns. While internal data provides a stable and reliable baseline, external data offers broader coverage but is more susceptible to inconsistency.

³ In preparation for our Annual Report 2025 we found an error in the production of our 2024 total application volume figures, in which we incorrectly published financial year figures instead of calendar year figures. This has now been corrected.

Table 12.12: Decisions of applications submitted to IPCO, 2020 to 2025

	Of which				
	Decisions made	Authorised	Returned	Rejected	Withdrawn
2020	223,322	199,482	23,596	244	3,051
2021	242,535	222,009	20,244	282	2,736
2022	266,755	245,125	21,529	100	4,087
2023	295,904	273,099	22,688	117	6,053
2024	320,539	291,345	29,129	65	8,558
2025	349,280	316,961	32,163	156	9,459

12.33 The rate for applications returned for rework has varied between 7.7% and 10.6% of all decisions since 2020. In 2025, the rate was 9.2% of all decisions, increasing from 9.1% in 2024.

12.34 The number of applications we returned for rework during 2025 was an illustration of the level of scrutiny that was applied to every application and the data shown below provides assurance that our high standard of case consideration has remained consistent.

12.35 Table 12.13 highlights that the primary reason for returning an application to the submitting authority was that an Authorising Individual assessed the application did not meet the necessity requirements. Some of the other reasons given were more technical in nature but all related in some way to inadequacy or lack of clarity in the information provided in the application. We regularly share information on Return for Rework (RfR) with law enforcement and public authorities to help them improve the quality of applications.

Table 12.13: Return for Rework (RfR) reasons, 2020 to 2025

Reason	2020	2021	2022	2023	2024	2025
Necessity	2,832 12%	4,389 18%	4,720 17%	4,471 14%	8,320 18%	8,918 23%
Other (up to 21 categories)	5,663 24%	4,183 17%	4,183 15%	7,285 22%	10,112 22%	7,525 19%
Proportionality	2,832 12%	2,988 12%	4,135 15%	4,458 14%	5,710 12%	5,376 14%
Consequential²	3,540 15%	3,188 14%	3,796 14%	2,652 8%	4,704 10%	5,525 14%
Dates/Times	2,596 11%	3,516 15%	3,669 13%	4,066 13%	4,752 10%	3,061 8%
Accuracy	1,652 7%	1,922 8%	1,725 6%	2,665 8%	3,639 8%	2,370 6%
Forward facing	944 4%	952 4%	1,025 4%	1,867 6%	2,466 5%	2,181 6%
Attribution	1,416 6%	1,244 5%	1,657 6%	2,576 8%	3,082 7%	2,047 5%
Collateral intrusion	1,180 5%	1,000 4%	1,592 6%	1,267 4%	2,005 4%	1,045 3%
Data Type	944 4%	587 2%	695 3%	1,108 3%	1,395 3%	849 2%
Total	23,599 100%	23,969 100%	27,197 100%	32,415 100%	46,185 100%	38,897 100%

Notes:

¹ Applications can be returned for rework for more than one reason. Therefore, the total number of RfR reasons exceeds the number of applications returned in table 12.12.

² Consequential now includes consequential ticked/unticked and consequential justification.

Bulk powers

12.36 Table 12.14 shows the number of authorisations (including renewals) for each class of bulk warrant since 2019.

Table 12.14: Bulk warrants and renewals by type, 2019 to 2025

Year	2019	2020	2021	2022	2023	2024	2025	Trend
Bulk equipment interference	10	12	13	16	23	29	37	
Bulk interception	30	31	33	30	26	27	25	
Bulk communications data	18	14	14	24	21	24	16	
Bulk personal data – specific	85	76	66	77	83	69	48	
Bulk personal data – class	101	108	111	111	114	98	58	
Bulk Personal dataset – Part 7A							31	
Bulk Personal dataset – Part 7B							34	

Note:

The number of BPD applications for 2025 are fewer than in previous years as the renewal period was extended from 6 to 12 months from November 2024, therefore less applications were made to IPCO.

Bulk personal datasets – Part 7A

12.37 In 2025, 31 applications were made for a bulk personal dataset (BPD) authorisation under Part 7A of the IPA, including new individual and category authorisations, renewals and urgent cases.

12.38 This included 10 applications for new category authorisations, of which Judicial Commissioners approved four, with six applications being withdrawn.

Bulk personal datasets – Part 7B

12.39 In 2025, 38 applications were made for third party BPD warrants under Part 7B of the IPA, including new applications, renewals and urgent cases. Of these, four were granted in urgent cases.

12.40 Of the 38 applications made, Judicial Commissioners refused to approve four.

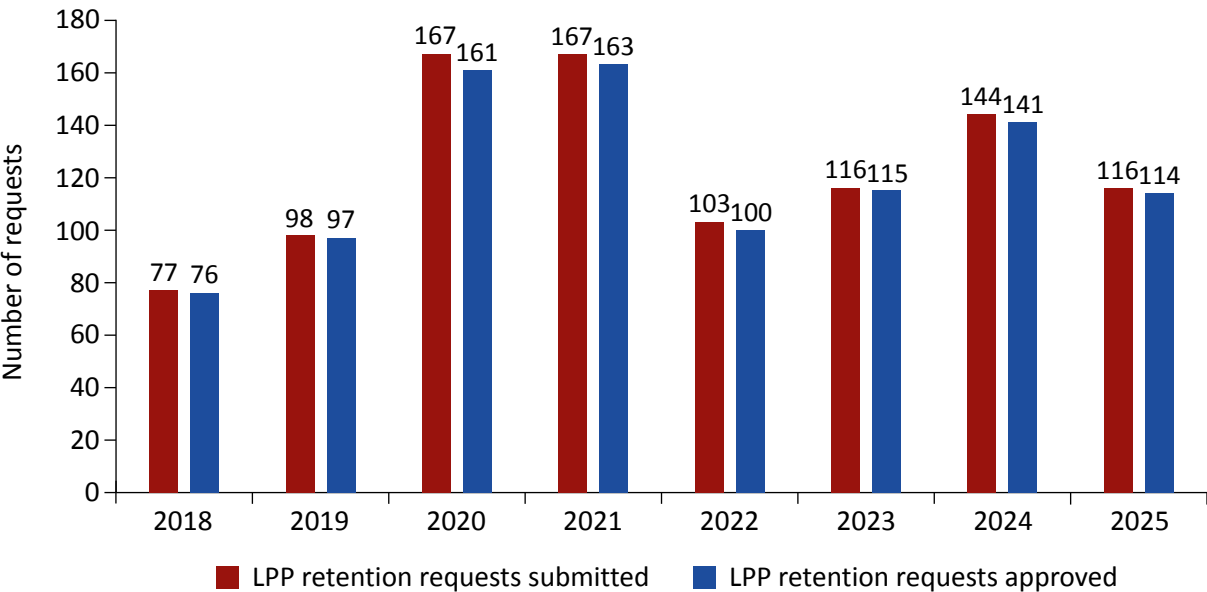
Confidential or journalistic information

12.41 The Investigatory Powers Act 2016 (Remedial) Order 2024 brought in the requirement to obtain authorisation from a Judicial Commissioner prior to an analyst selecting for examination bulk interception content where the purpose was to acquire confidential journalistic material or identify a source of journalistic information (or where this was highly likely). In 2025, there were 14 authorisations for such content. The Investigatory Powers (Amendment) Act 2024 (IP(A)A) introduced a similar requirement for bulk equipment interference and in 2025, Judicial Commissioners made 16 authorisations relating to such content.

Legal professional privilege (LPP) material

12.42 Public authorities must inform us if they think it is necessary to retain LPP material and apply to a Judicial Commissioner for permission to do so. In 2025, we approved 114 requests from 116 applications.

Figure 12.10: Number of requests submitted and approved for LPP material, 2018 to 2025



Notices

12.43 The IPA introduced the power for the Secretary of State to issue notices to telecommunications operators to assist public bodies and agencies working under the Act. There are three types of notices: Data Retention Notices; Technical Capability Notices; and National Security Notices.

12.44 In 2025, Judicial Commissioners considered notices in accordance with the statutory framework, providing independent scrutiny and written reasons where appropriate.

Intelligence Services Act 1994

12.45 Section 5 of the Intelligence Services Act 1994 (ISA) relates to interference with property or wireless telegraphy by the intelligence agencies. In 2025, 565 section 5 warrants were granted by the Secretary of State (these are not subject to Judicial Commissioner approval).

12.46 Section 7 of the ISA applies to acts done outside the UK and which are necessary for the proper discharge of a function of the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) only. In 2025, 91 section 7 warrants were issued by the Secretary of State (these are not subject to Judicial Commissioner approval, but are subject to inspection).

The Principles

- 12.47 “The Principles relating to the Detention and Interviewing of Detainees Overseas and the Passing and Receipt of Intelligence Relating to Detainees” (The Principles) is a published government policy relating to how the intelligence agencies, the Ministry of Defence (MoD), the National Crime Agency (NCA) and Counter-Terrorism Police (CTP) London must deal with detainees and intelligence relating to detainees overseas, outside UK jurisdiction. The Principles came into effect on 1 January 2020 and replaced the Consolidated Guidance. The Principles provide guidance in support of the UK Government’s position that it does not participate in, solicit, encourage or condone unlawful killing, the use of torture or cruel, inhuman or degrading treatment (CIDT) or extraordinary rendition.
- 12.48 Table 12.15 sets out the total number of cases in which the Principles Partners have referred to Ministers for a decision because there was a real risk of occurrence of one or more of the categories of unacceptable conduct as set out in The Principles. They also include the number of cases which the Partners have proactively brought to our attention because they raised particular legal or policy issues – some of which have informed the findings presented in this report.
- 12.49 As in previous years, there are important caveats to the data presented here:
- First, an increase in cases which cross the threshold of real risk does not necessarily indicate that the Principles Partners have taken additional risks in their engagement with overseas authorities. A single operation (for example, in response to a major terrorist plot) may generate a spike in referrals to Ministers. 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 Principles has increased. Similarly, a reduction in the number of cases does not necessarily suggest a lower risk appetite has been adopted.
 - Secondly, as The Principles makes clear, consulting Ministers does not imply that action will or will not be authorised.

Table 12.15: Cases reviewed under The Principles, 2020 to 2025

Number of cases reviewed		2020	2021	2022	2023	2024	2025
Cases reviewed on inspection		93	68	104	85	101	100
Cases reviewed proactively due to contentious legal or policy issues		8	7	7	2	1	3
Triggers: Total number of all cases (not limited to those reviewed on inspection)	Personnel knew or believed torture, unlawful killing or extraordinary rendition would occur	0	0	0	0	0	0
	Personnel identified a real risk of torture, unlawful killing or extraordinary rendition and submitted for approval despite the presumption not to proceed in such cases (this may include cases where engagement is intended to reduce the risks of unacceptable conduct or where there is an imminent threat of serious harm to individuals including children)	2	3	8	3	9	9
	Personnel identified a real risk of CIDT and submitted for approval	15	17	17	22	22	35
	Personnel identified a real risk of rendition and submitted for approval	3	0	0	0	0	1
	Personnel identified a real risk of unacceptable standards of arrest and/or detention and submitted for approval	28	34	54	45	50	85

12.50 It is important to note that, in respect of The Principles, our oversight concerns the process which informs a Minister's decision; however, unlike in other aspects of our work, we do not review the Minister's decision itself on judicial review grounds. The IPC does not consider it within his remit to present statistics on areas that are outside of his direct oversight and has decided that the current data presented in the Annual Report in respect of our oversight of The Principles is appropriate. The operation of The Principles is complex and providing meaningful statistics that demonstrate how the policy has been used without divulging details of specific cases has always been a difficult balance to strike and we will continue to keep their presentation under review.

The UK-US Data Access Agreement

12.51 In 2025, Judicial Commissioners conducted additional reviews of 4,437 necessity and proportionality statements for relevant targeting decisions when an individual is targeted for the first time under a general descriptor on a thematic TI warrant and targeted CD authorisations for the purpose of acquiring data pursuant to the UK-US Data Access Agreement (see IPCO Advisory Notice 1/2023).⁵² The number of additional reviews does not reflect the number of times a new targeting decision under the UK-US Data Access Agreement is made. This is because an additional review is not required where an individual is named under a targeted warrant or added to a thematic warrant by way of major modification.⁵³

⁵² See: [Advisory-Notice-1_2023-UK-US-DAA-Advisory-Notice-13-February-2023-4.pdf](#)

⁵³ See: from paragraph 4.69 for more details.

Annex A. Definitions and glossary

Annex A is divided into three parts:

- definitions of terms about the use and oversight of investigatory powers;
- a glossary of the authorities we oversee; and
- a summary of the abbreviations used throughout the report.

Definitions

Term	Definition
Bearer	A communication link carrying data e.g., Internet Protocol data.
Bulk communications data	This is communications data relating to a large number of individuals; communications data is the information about a communication but not the content. It includes the “who”, “where”, “when”, “how” and “with whom” of a communication. This could be a list of subscribers to a telephone or internet service, for example.
Bulk interception	Bulk interception allows for the collection of communications of persons who are outside the UK. This enables authorities to discover threats that may otherwise be unidentified.
Bulk personal data	Bulk personal datasets are electronic sets of personal information about a large number of individuals, for example, an electoral roll or telephone directory. Although the data held is on a large group of people, analysts will only actually look at data relating to a minority who are of interest for intelligence purposes.
Code of Practice	A Code of Practice provides guidance to public authorities on the procedures to be followed when they use investigatory powers. The advice offered in any Code of Practice takes precedence over any public authority’s own internal advice or guidance. In general, there are separate Codes of Practice available for each power. These are available on the GOV.UK website

Term	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. An example of this would be the unintentional recording of background conversation of passers-by alongside the speech of the target. Additional intrusion to the privacy of the passers-by would have taken place – this is collateral intrusion. We expect public authorities proactively to assess the possible extent of collateral intrusion in any proposed activity and, where possible, take reasonable steps to prevent this.
Communications data	Communications data is the “who”, “where”, “when” and “how” of a communication but not its content. It enables the identification of the caller, user, sender or recipient of a phone call, text message, internet application or email (together with other metadata), but not what was said or written. In addition to electronic communications, it also covers postal services, enabling the identification of a sender or recipient of a letter or parcel.
Covert human intelligence sources	A covert human intelligence source (informally referred to as a “CHIS”) is an informant or an undercover officer. They support the functions of certain public authorities by providing intelligence covertly. A CHIS under the age of 18 is referred to as a juvenile CHIS. “Relevant source” is the term used to describe staff from a designated law enforcement agency that are trained to act as undercover operatives and are subject to an enhanced authorisation and oversight regime. A CHIS may be authorised to participate in criminal conduct in specific circumstances, namely in the interests of national security; for the purpose of preventing or detecting economic crime or of preventing disorder; or in the interests of the economic well-being of the United Kingdom.
Covert surveillance	Surveillance is covert if it is carried out in a manner that ensures the subject of the surveillance is unaware that it is or may be taking place. Surveillance includes monitoring, observing or listening to people, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.
Directed surveillance	This is surveillance that is covert but not carried out in a residence or private vehicle. It could include the covert monitoring of a person’s movements, conversations and other activities.

Term	Definition
Double lock	Public authorities must have authorisation to use the most intrusive investigatory powers. Authorities will therefore submit applications for the use of investigatory powers to a Secretary of State or a senior officer; this decision is then reviewed and authorised by one of our Judicial Commissioners. Other than in urgent circumstances, only with authorisation from one of our Judicial Commissioners can a warrant be issued. This is the double lock process. It ensures a two-stage approval for the use of investigatory powers.
Equipment interference	Equipment interference is the process by which electronic equipment may be interfered with to obtain stored communications or other information. Activity could include remote access to a computer or covertly downloading a mobile phone's contents.
Interception	Interception is the process that makes the content of a communication available for examination by someone other than the sender or recipient of the communication. (NB: examination is the process by which material is selected to be read, looked at or listened to by the persons to whom it becomes available as a result of interception and could include listening to telephone calls or opening and reading the contents of a person's letters or emails).
Intrusive surveillance	This is surveillance which is carried out, for example, using eavesdropping devices in residential premises or in private vehicles. It may involve the covert presence of a listening device to capture conversations and ensure that the individual being observed is unaware that surveillance is taking place.
Modification	A modification is a change to a warrant authorising the use of investigatory powers. It is requested after the warrant has been issued. A modification to a warrant could be, for example, adding an additional individual so that their communications can be lawfully intercepted.
National Security Notice	Under section 252 of the Investigatory Powers Act 2016, a Secretary of State, with approval from a Judicial Commissioner, can issue a National Security Notice (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 additionally be authorised under a warrant. National Security Notices could, for example, ask a company to provide access to a particular facility.

Term	Definition
Operational purpose	The IPA established defined operational purposes for the use of BPD. An agency may only use bulk data for an operational purpose listed on the warrant under which the BPD is being retained and examined. Under the IPA, the full list of operational purposes is approved by the Prime Minister.
Promotion rules	These determine what intercepted data is forwarded to storage in order to make it available for selection for examination by analysts.
Property interference	Property interference is the covert interference with physical property, but also covers wireless telegraphy. This may be for the purpose of conducting a covert search or trespassing on land. For example, police may trespass to install a listening device covertly in a person's house.
Relevant Error	A relevant error is an error made by a public authority when carrying out activity overseen by IPCO. A relevant error is defined in section 231(9) of the Investigatory Powers Act 2016.
Section 7 of the Intelligence Services Act 1994	Section 7 of the Intelligence Services Act 1994 enables the Foreign Secretary to authorise activity by the intelligence agencies outside the UK that would otherwise be unlawful under UK domestic law.
Serious Error	Section 231(2) of the Investigatory Powers Act 2016 defines a serious error as one where significant prejudice or harm has been caused to an individual as a result of a relevant error.
Targeted interception	Targeted interception is the process that makes the content of a communication available to someone other than the sender or recipient. This could include listening to telephone calls or opening and reading the contents of a person's letters or emails.
Technical Capability Notice	Under section 253 of the Investigatory Powers Act 2016, the Secretary of State, with approval from a Judicial Commissioner, may issue a Technical Capability Notice (TCN) to require telecommunications or postal operators to ensure they are able to provide assistance with the acquisition of communications data, interception and equipment interference. After a Technical Capability Notice has been issued and implemented, a company can act quickly and securely when a warrant is authorised.

Term	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 major modification, which must be notified to a Judicial Commissioner. For equipment interference by law enforcement agencies, a major modification requires 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. For this 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) included within the general description of the subjects, although individual factors (such as their telephone numbers or email addresses) would be added by internally authorised minor modifications.
The Principles	“The Principles relating to the detention and interviewing of detainees overseas and the passing and the receipt of intelligence relating to detainees” are more commonly referred to as “The Principles”. These are published by the Cabinet Office and apply to the intelligence services, the National Crime Agency, the Metropolitan Police Service, the Armed Forces and the Ministry of Defence. The Principles are intended to ensure that the treatment of detainees overseas, and the use of intelligence on detainees, is consistent with the UK’s human rights and international law obligations. The document seeks to provide clear guidance to staff often operating in legally complex and challenging circumstances. The Principles came into force on 1 January 2020.

Term	Definition
Urgency provisions	Urgency provisions are the conditions under which, due to time-sensitive operational reasons (such as an imminent threat to life), legislation permits a departure from the normal authorisation process. For an investigatory power that typically needs to be subject to the “double lock”, the urgency provisions mean this can be used without a Judicial Commissioner’s approval in advance. If an urgency provision is used, the person who decided to issue a warrant to use the investigatory power must inform a Judicial Commissioner that it has been issued and the power has been used. A Judicial Commissioner must then either: • decide to approve the decision to issue the warrant and notify the authority of the Judicial Commissioner’s decision; or • decide to refuse to approve the decision, in which case activity under the warrant must stop and the Commissioner may direct that any information obtained under the urgent warrant be destroyed.
Wireless telegraphy	Wireless telegraphy refers to the conveying of information using electromagnetic energy with a frequency of less than 3,000 gigahertz.

Further details on the authorisation process for each of these powers can be found on our website.⁵⁴

54 See: The Powers – IPCO

Glossary of authorities

Intelligence Agencies	• Security Service (MI5) • Secret Intelligence Service (SIS) • Government Communications Headquarters (GCHQ) References to “UKIC” mean the United Kingdom intelligence community.
Defence	Ministry of Defence
Law Enforcement Agencies (LEAs)	• 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 • His Majesty's Revenue and Customs (HMRC) • National Crime Agency (NCA) • The Home Office (Border Force and Immigration Enforcement)
Wider Public authorities (WPAs)	• 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 and Trade (Insolvency Service) • 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 Accidents 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) • 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 • His Majesty's Chief Inspector of Education, Children's Services and Skills (OFSTED) • His 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 • Ministry of Housing, Communities and Local Government (MHCLG) • National Anti-Fraud Network (NAFN) • National Health Service (NHS) Business Services Authority • National Health Service (NHS) Counter Fraud Authority • Natural Resources Wales • Department of Justice in Northern Ireland (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 Group • 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 • UK National Authority for Counter Eavesdropping (UKNACE) • Welsh 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

Abbreviations

AA	Automatic acquisition
ACCIPIF	Authorised Communications Controls and Interception Policy Frameworks
AI	Artificial intelligence
AI	Authorising individual
ACL	Access control levels
AO	Authorising officer
APCC	Association of Police and Crime Commissioners
BCD	Bulk communications data
BEI	Bulk equipment interference
BI	Bulk interference
BPD	Bulk personal dataset
CAB	Covert Authorities Bureau
CCA	Criminal Conduct Authorisations
CDR	Call data records
CETA	Centre for Emerging Technology and Security
CFU	Counter Fraud Unit
CHIS	Covert human intelligence sources
CIDT	Cruel, inhuman or degrading treatment
CJEU	Court of Justice of the European Union
CMA	Computer Misuse Act 1990
CMS	Case Management System
CMT	Compliance Monitoring Team
CoA	Court of Appeal
COM	Covert Operations Manager
CNE	Computer Network Exploitation
CoP	Code of Practice
COPO	Crime (Overseas Production Orders) Act 2019
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service

CSA NS	Chief Scientific Advisor for National Security
CSP	Communications service provider
CST	Council for Science and Technology
CTOC	Counter Terrorism Operations
CTP	Counter Terrorism Police
DAA	Data Access Agreement
DCMS	Digital Culture, Media and Sports
DIPC	Deputy Investigatory Powers Commissioner
DPA	Data Protection Act 2018
DSA	Directed surveillance authorisation
DSO	Designated Senior Officer
DSU	Dedicated Source Unit
DV	Developed vetting
ECHR	European Convention on Human Rights
EIO	European Investigation Order
EION	European Intelligence Oversight Network
ERS	Error Reduction Strategy
2FA	Two-Factor Authorisation
FACT	Federation against Copyright Theft
FIORC	Five Eyes Intelligence Oversight Review Council
FOIA	Freedom of Information Act 2000
FSA	Finite State Automata
HMGCC	His Majesty's Government Communications Centre
HOIE	Home Office Immigration Enforcement
ICR	Internet Connection Records
IIOC	Indecent images of children
IP	Internet protocol
IPA	Investigatory Powers Act 2016
IP(A)A	Investigatory Powers (Amendment) Act 2024
IPAR	Internet Protocol Address Resolutions

IPC	Investigatory Powers Commissioner
IPCO	Investigatory Powers Commissioner's Office
IPT	Investigatory Powers Tribunal
ISA	Intelligence Services Act 1994
JC	Judicial Commissioner
KET	Knowledge Engagement Team
LEA	Law Enforcement Agency
LPP	Legal professional privilege
LTHSE	Long-Term High Security Estate
ML	Machine Learning
MoU	Memorandum of Understanding
NAFN	National Anti-Fraud Network
NCDS	National Communications Data Service
NCMEC	National Centre for Missing and Exploited Children
NCND	Neither confirm nor deny
NPCC	National Police Chiefs' Council
NSIRA	National Security and Intelligence Review Agency
NSWG	National Source Working Group
NTAC	National Technical Assistance Centre
NUWG	National Undercover Working Group
NFC	Near field communications
NGO	Non-governmental organisation
OCDA	Office for Communications Data Authorisations
OpSy	Operational Security Officer
OSJA	Overseas Security and Justice Assistance
PCC	Police and Crime Commissioner
PET	Privacy Enhancing Technology
PIC	Participation in crime
PIO	Police Prison Intelligence Officers
PSI	Prison Service Instruction

RA	Requesting Agencies
RAA	Request Application Authorisation
REPHRAIN	National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online
RN	Retention notice
RfRs	Returns for Rework
RIPA	Regulation of Investigatory Powers Act 2000
RIP(S)A	Regulation of Investigatory Powers (Scotland) Act 2000
ROCUs	Regional Organised Crime Unit
RPM	Records Product Management
RRD	Retention, review and deletion
SAO	Senior Authorising Officer
S4E	Selection for examination
SLE	Service Level Expectation
SIS	Secret Intelligence Service
SIO	Senior Investigating Officer
SOI	Subject of Interest
SOP	Standard operating procedure
SOU	Special operations unit
SLE	Service level expectations
SPoC	Single Point of Contact
SRO	Senior Responsible Officer
SVAP	Security Vetting Appeals Panel
TAP	Technology Advisory Panel
TI	Targeted Interception
TEI	Targeted Equipment Interference
TIDU	Technical Intelligence Development Unit
TSU	Technical Surveillance Unit
TO	Telecommunications operator
UCPI	Undercover Policing Inquiry
UTC	Universal co-ordinated time

UKDA	UK Designated Authority
UKIC	UK Intelligence Community
WGD	Warrant Granting Departments
WPA	Wider Public authority
ZKP	Zero Knowledge Proofs

Annex B. Budget

The table below gives a breakdown of the financial statement for the Investigatory Powers Commissioner's Office (IPCO) for the financial year 2025/26.

Budget total: £15.3million	
Period: 1 April 2025 to 31 March 2026	
	Full year outturn
Pay costs	£11,341,217
Travel and subsistence	£348,205
Office supplies and services	£32,661
Training and recruitment	£9,013
Estates	£661,222
IT and communications	£1,356,056
Legal costs (including consultancy)	£109,258
Other costs and services	£93,603
Capital costs	£1,148,118
Total	£15,099,353

Overview

For the financial year 2025/26, we reported total expenditure of £15.1 million against an approved budget allocation of £15.3 million. This comprised £13.1 million of resource expenditure (RDEL) and £2.2 million of capital expenditure (CDEL).

Pay costs

Pay expenditure for 2025/26 remained the most significant element of our overall spend. This includes staffing costs for civil servants, Judicial Commissioners and members of the Technology Advisory Panel (TAP).

Pay costs increased compared to the previous financial year, primarily due to the implementation of the 2025/26 pay award, which delivered a significant uplift to staff salaries. These increased costs were managed within the approved resource allocation and consistent with public sector pay policy.

Travel and subsistence

Expenditure on travel and subsistence was lower than the amount spent in 2024/2025. This reduction reflects the continued application of spending controls alongside the expanded use of remote inspection models and digital systems, which reduced the requirement for in-person inspections while maintaining operational delivery.

Estates

Total estates expenditure was lower than previous financial years. This reduction was driven by rental discounts agreed as part of lease renewals, resulting in improved value for money across IPCO's estates.

Legal costs

Our increase in legal expenditure was primary attributable to costs on external legal counsel in support of IPCO's statutory responsibilities. Costs rose significantly due to the Agent X investigation, which IPCO was directed to undertake by the Prime Minister, and which required specialist legal advice and representation during 2025/26. All costs for the Agent X investigation were covered by the Home Office and will continue to be covered by the Home Office in 2026/27.

Capital expenditure

Capital expenditure for the year totalled £1.15 million, against an approved capital budget of £2.2 million. Most of the capital spend related to improving our warrant management system and supporting our long-term digital capability.

Annex C. Serious errors

In 2025, the Investigatory Powers Commissioner (IPC) decided that the following errors would be investigated as potential serious errors within the meaning of section 231 of the Investigatory Powers Act 2016 (IPA).

Error investigation 1

	Public authority
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Subscriber records
Description:	In early 2025, an investigation into sexual communications with a child led to the seizure of multiple mobile devices. Examination of the devices revealed communication identifiers linked to potential child contacts. An application to obtain subscriber data contained a manual transcription error, resulting in the acquisition of subscriber details for an unrelated individual. This person was later contacted and interviewed as a potential witness. The error was subsequently identified, acknowledged, and corrected, with records updated and the affected individual informed. A further, corrected application enabled the identification of a child who disclosed having received an indecent image several months earlier; no ongoing contact or additional safeguarding concerns were identified. Therefore, we were satisfied that the delay arising from the error did not cause the victim significant prejudice or harm and, accordingly, concluded that no serious error occurred.
Consequence:	We assessed that the incident arose from human error during the initial application process and that no significant harm was suffered by the victim or the person contacted as a potential witness.

Error investigation 2

	Public authority
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Online username
Description:	Police sought Communications Data (CD) on four online usernames linked to the sharing of indecent images of children. In one, a number at the end of the username was mistakenly omitted. No checks were made to confirm the accuracy of the data and a request to arrest a suspect was made to a neighbouring police force.
Consequence:	A person was arrested and detained for questioning. It was only after the person had been released on bail did the police identify the error. The arrest would likely have been avoided by adherence to the error reduction strategy. The Investigatory Powers Commissioner (IPC) decided that this error amounted to a serious error (within the meaning of section 231 of the IPA). Accordingly, the IPC notified the affected person of the facts and their right to apply for a right of remedy via the Investigatory Powers Tribunal (IPT).

Error investigation 3

	Public authority
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Online username
Description:	Police seeking to locate a wanted person sought to identify the subscriber of an online username thought to be used by that individual. Communications Data (CD) was acquired upon the username and a series of locations were searched by police. Further investigation revealed the subscriber of the username obtained was unconnected to the wanted person and the identification had been based on flawed analysis.
Consequence:	In one of the properties visited, the occupants, having no knowledge of the wanted person, declined to allow the police access. Upon refusal the police exercised powers to search the property under section 17 of the Police and Criminal Evidence Act. The search was negative. The IPC decided that this error amounted to a serious error (within the meaning of section 231 of the IPA). Accordingly, the IPC notified the affected persons of the facts and their right to apply for a right of remedy via the Investigatory Powers Tribunal.

Error investigation 4

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect data
Data Acquired:	Internet Protocol Address Resolutions (IPARs)
Description:	In early 2025, we were advised of a discrepancy in CD linked to devices accessing the internet via a specific mobile network. Following a system change in how the time of this activity is recorded and analysed, a series of false positives (72) and false negatives (88) were identified.
Consequence:	A false positive gave the requesting authority details of a single device when a zero result should have been provided. The potential for a serious error to occur was therefore high. In most cases other evidence was able to corroborate the initial data. In two cases where no corroboration was available, this led to the arrest of two innocent persons. A false negative gave the requesting authority a zero result when in fact details of a single device should have been provided. This delayed investigations though most investigations were progressed using other corroborative evidence. A Telecommunications Operator (TO) cannot make a relevant error under the IPA. The matter was therefore referred to the Information Commissioners Office for consideration.

Error investigation 5

	Telecommunications operator (TO)
Human or Technical:	Technical
Classification:	Incorrect data
Data Acquired:	MSISDN (telephone number)
Description:	A call was made to a police force by a person threatening significant harm to local people. CD was obtained from a TO covering the time the call was made to the police control room. Investigation established police had correctly requested CD for British Summer Time. The TO however provided details of the call in Greenwich Mean Time (60 minutes earlier).
Consequence:	The details provided by the TO led to the arrest of an innocent caller. When interviewed the arrested person provided evidence of making a call to the police 60 minutes earlier over a traffic matter. A TO cannot make a relevant error for the purposes of this legislation. The matter was therefore referred to the Information Commissioner's Office for consideration.

Error investigation 6

	Telecommunications operator (TO)
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Subscriber records – internet services
Description:	A police force investigating offences involving the distribution of indecent images of children was granted authority to identify the user of an IP address. The TO returned data relating to the relevant account but highlighted a discrepancy between the billing address and the installation address. The TO could not provide a reason for the discrepancy but warned against relying on the data as its accuracy could not be confirmed.
Consequence:	The police decided action needed to be taken due to the nature of the offences involved and visited the installation address to speak with the occupants. The occupants were eliminated from enquiries and a visit to the second address (listed as the billing address) resulted in a suspect being arrested and admissions made. The true cause of the discrepancy was never established but we believe it was likely a transposition error on the TO account records (the two address were in the same road a few doors apart, with similar house numbers). We questioned whether the police could have undertaken further checks to determine which of the two properties was the correct address. However, after investigation it was determined that the potential checks available would have been inconclusive and a visit to both addresses would still have been needed. A TO cannot make a relevant error under the IPA. The matter has been referred to the Information Commissioner's Office for consideration and the occupants of the first address made aware of the police complaints procedures.

Error investigation 7

	Telecommunications operator (TO)
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Internet Protocol Address Resolutions (IPARs)
Description:	Six police forces sought IPARs from a TO. A new retention system under test was inadvertently used to provide the data. The system should not have been used operationally while testing was ongoing.
Consequence:	In all six cases the police force analysed the results against other corroborative material. All identified the inaccuracy in the dataset and made contact to advise the TO the data they provided was incorrect. This was a textbook response by the police forces concerned to identify an error before enforcement action was considered. As a result, no innocent person was affected.

Error investigation 8

	Telecommunications operator (TO) and public authority
Human or Technical:	Human
Classification:	Incorrect data
Data Acquired:	Subscriber records
Description:	In 2025, it was identified that two relevant errors had occurred in 2023 but were not recognised as such at the time due to complex ongoing investigations by the public authority to determine the cause of the issue. Both cases related to the same overseas TO and involved offences concerning the online possession of indecent images of children. Subsequent information identified a systemic data-quality issue affecting how certain IP address fields were populated, creating a risk that IP data associated with user registration was inaccurate.
Consequence:	Though guidance was issued advising investigators to exercise caution; CD was nonetheless sought and disseminated using the affected IP information, resulting in investigative activity based on potentially flawed data. In one case the investigative activity resulted in an innocent person being arrested and detained for questioning. In a further case, three generations of the same family were visited at separate addresses and questioned by police seeking to identify a potential suspect. In both cases the IPC decided that the failures to heed the warnings provided by the TO constitute a failing in the requirement to maintain integrity of the process in place within a public authority to acquire CD and therefore amounted to a serious error (within the meaning of section 231 of the IPA). Accordingly, the IPC notified the affected persons of the facts and their right to apply for a right of remedy via the Investigatory Powers Tribunal.

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