



HM Government

HM Government Transparency Report 2017: Disruptive and Investigatory Powers



HM Government Transparency Report 2017: Disruptive and Investigatory Powers

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

February 2017



© Crown copyright 2017

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

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

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

Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gsi.gov.uk

Print ISBN 9781474140935

Web ISBN 9781474140942

ID 09021701 02/17 58597

Printed on paper containing 75% recycled fibre content minimum

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

Contents

| | | |
|----------|----------------------------------------------------------------------------------|-----------|
| 1 | Foreword | 5 |
| 2 | Introduction | 7 |
| 3 | Terrorism Arrests and Outcomes | 9 |
| 4 | Serious and Organised Crime Arrests and Outcomes | 13 |
| 5 | Disruptive Powers | 15 |
| 5.1 | Stops and Searches | 15 |
| 5.2 | Port and Border Controls | 16 |
| 5.3 | Terrorist Asset-Freezing | 18 |
| 5.4 | Terrorism Prevention and Investigation Measures | 21 |
| 5.5 | Royal Prerogative | 23 |
| 5.6 | Seizure & Temporary Retention of Travel Documents | 24 |
| 5.7 | Exclusions | 24 |
| 5.8 | Temporary Exclusion Orders | 25 |
| 5.9 | Deprivation of British Citizenship | 25 |
| 5.10 | Deportation with Assurances | 26 |
| 5.11 | Proscription | 27 |
| 5.12 | Closed Material Procedure | 29 |
| 5.13 | Tackling Online Extremism | 30 |
| 5.14 | Tackling Online Child Sexual Exploitation | 31 |
| 6 | Investigatory Powers | 33 |
| 6.1 | Investigatory Powers Act 2016 | 33 |
| 6.2 | Overview of Interception | 34 |
| 6.3 | 8(1) Warrants | 36 |
| 6.4 | 8(4) Warrants | 37 |
| 6.5 | Targeted Communications Data | 39 |
| 6.6 | Bulk Communications Data Acquisition | 45 |
| 6.7 | Covert Surveillance, Covert Human Intelligence Sources and Property Interference | 49 |
| 6.8 | Equipment Interference | 53 |
| 6.9 | Investigation of Protected Electronic Information | 54 |
| 6.10 | Bulk Personal Datasets | 56 |

| | |
|----------------------------------------------------------------------|------------|
| 7 Oversight | 59 |
| 7.1 Independent Reviewer of Terrorism Legislation | 60 |
| 7.2 Interception of Communications Commissioner | 62 |
| 7.3 Intelligence Services Commissioner | 69 |
| 7.4 Office of Surveillance Commissioners | 73 |
| 7.5 Investigatory Powers Tribunal | 75 |
| 8 Recommended Reading List | 79 |
| 9 Annexes | 83 |
| Annex A: Terrorist Asset-Freezing Figures | 83 |
| Annex B: Proscribed Organisations | 85 |
| Annex C: Items of Communications Data by Public Authority | 103 |
| Annex D: IPT Decisions, 2011-2015 | 108 |

Foreword



The Government is committed to increasing the transparency of the work of our security and intelligence and law enforcement agencies. This Government has gone further than ever before to put information in the public domain about the activity undertaken by these agencies to keep the public safe. I am pleased to be able to continue that process with the publication of this Transparency Report.

Since the last Report was published in 2015, the Government has continued to keep the public as informed as they can be about the way in which the agencies undertake their investigations, and the ways in which terrorists and serious criminals are disrupted. The Investigatory Powers Act 2016, given Royal Assent on 29 November, is an excellent example of this. The Act brings together powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. And it makes these powers – and the safeguards that apply to them – clear and understandable.

The passage of this legislation through Parliament saw more information about the work of the agencies put in to the public domain than ever before. This included extensive material produced by the Government to set out the operational case for the powers in the Act. Furthermore, we also asked David Anderson QC to conduct a comprehensive review of the operational case for bulk powers. This review was published in full, with no confidential annexes, and provides the public with unprecedented detail about why the bulk powers in the Act are of crucial importance. David Anderson has since described the Act as introducing “world-leading standards of transparency”.


This activity shows that where we can give the public more information, we do. However, we recognise that more can be done. In particular, we must ensure that we do not just have a transparent legal framework, but that we also provide the public as much information as possible about how that framework is utilised by the agencies charged with the vital task of investigating crime and protecting our national security. That is why we committed to produce this important report on a regular basis.

This is the second edition of this report and, as was the case in the last report, it provides a consolidated picture of the use, regulation and oversight of a wide range of disruptive and investigatory powers that are crucial to protecting the public from those that would do us harm.

The report explains to the public information that has already been made available, both in relation to the threats that we face and what we do to counter them. It provides extensive statistical information about the various disruptive and investigatory powers used by our

law enforcement and security and intelligence agencies. And it builds on that statistical information, compiling in one place a detailed explanation of how these powers are used, why they are important and, crucially, how their use is safeguarded and overseen.

It is through this process that we can give the public a true understanding of the range of tools that are available to our law enforcement and security and intelligence agencies, and the role those tools play in defending our national security.

A handwritten signature in black ink, appearing to read 'Amber Rudd'.

Amber Rudd MP
Home Secretary

2 – Introduction

The 2015 National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) set out the Government's vision for an integrated approach to countering terrorism, using the full spectrum of capabilities across security, defence, diplomacy and development. The SDRS included a commitment to update CONTEST, the United Kingdom's Strategy for Countering Terrorism, in 2016.

We have reviewed CONTEST to ensure the highest priorities are given the right resources, and that Government departments and agencies have a unified approach. A new version of CONTEST will be published shortly.

The latest CONTEST Annual Report to Parliament,¹ was published on 21 July 2016. The report makes clear that the UK faces a significant and changing terrorist threat, in particular from Daesh, its affiliates and individuals inspired by Daesh. 12 plots in Great Britain have been successfully disrupted by the police and the security and intelligence agencies since June 2013.

As a result of this threat, the UK threat level, set by the Joint Terrorism Analysis Centre, has remained at 'SEVERE' since 29 August 2015, meaning an attack in the UK is highly likely.

The UK also faces threats from Al Qa'ida's senior leadership which, despite having been weakened, has not gone away. Alongside the threat from Islamist terrorists, there is an ongoing threat from Northern Ireland Related Terrorism. The threat of violence and terrorism from groups and individuals associated with the far and extreme right wing is growing.

Equally, serious and organised crime continues to constitute a threat to our national security. The 2015 Annual Report on the Government's Serious and Organised Crime Strategy was published on 23 March 2015 and the latest National Strategic Assessment of Serious and Organised Crime was published on 9 September 2016. Serious and organised crime costs the United Kingdom at least £24 billion each year, leads to loss of life and can deprive people of their security and prosperity. Organised crime is wide ranging and includes drugs trafficking, human trafficking, high value fraud, other financial crime and cyber-crime. Serious crime is that which demands a national coordinated response, notably fraud and child sexual exploitation. These crimes damage communities, destabilise financial markets, threaten the security of our borders and undermine confidence in communications technology and the online economy.

¹ This report should be read in conjunction with "CONTEST, the United Kingdom's Strategy for Countering Terrorism" and "HM Government Serious and Organised Crime Strategy". The use of the powers outlined in this report form a fundamental part of these strategies. The strategies, as well as the Annual Reports on the operation of CONTEST, are available at www.gov.uk.

Hostile state activity, including espionage, also continues to pose a threat to British interests. Cyber espionage in particular has posed an increasing threat over recent years, with new technologies enabling espionage to take place on an almost industrial scale in some cases. The 2015 NSS reaffirmed the cyber threat as one of the most significant risks to UK interests. The NSS set out the Government's determination to address cyber threats and put in place tough and innovative measures as a world leader in cyber security. To deliver on that commitment, in November 2016 the Government published the 2016-2021 National Cyber Security Strategy. The National Cyber Security Centre, which was launched in October 2016, is a key means for government to deliver many elements of strengthened cyber security for the UK.

In light of the variety of threats the UK faces, it is crucial that we have the powers we need to effectively counter them, and that they are used appropriately and proportionately.

This is the second issue of the Government's Transparency Report, which explains the tools the Government, law enforcement, and the security and intelligence agencies use to counter terrorism, serious and organised crime, and state-based threats.

The report is split into two main sections. The first includes figures on the use of disruptive and investigative powers. It explains their utility and outlines the legal frameworks that ensure they can only be used when necessary and proportionate, in accordance with the statutory functions of the relevant agencies. The second section explains the roles of the Commissioners, and other bodies, who provide independent oversight and scrutinise the use of these tools.

There remain limits to what can be said publically about the use of certain sensitive techniques, and particularly the work of the intelligence agencies, because to go further could encourage criminals and terrorists to change their behaviour in order to evade detection.

However, it is vital the public are confident that the intelligence and law enforcement agencies have the powers they need to protect the public and that they are used proportionately. These agencies rely on many members of the public to provide support to their work. If the public do not trust the police and intelligence agencies, that mistrust would have a real operational impact.

This report therefore ensures that the public are able to access, in one place, a comprehensive guide to the powers used to combat threats to the security of the United Kingdom, the extent of their use and the safeguards and oversight in place to guard against their misuse.

3 – Terrorism Arrests and Outcomes

Conviction in a court is one of the most effective tools we have to stop terrorists. The Government is therefore committed to pursuing convictions for terrorist offences where they have occurred. Terrorism-related arrests are made under the Police and Criminal Evidence Act 1984 (PACE). They can also be made under the Terrorism Act 2000 (TACT) in circumstances where arresting officers require additional powers of detention or need to arrest a person suspected of terrorism-related activity without a warrant. Whether to arrest someone under PACE or TACT is an operational decision to be made by the police.

In the year ending 30 September 2016, 255 persons were arrested for terrorism-related offences, a decrease of 20% from the 317 arrests the previous year. This reflects a particularly high number of arrests in two of the quarters in the year to September 2015. Therefore although the number of arrests fell in this period, it is still relatively high when compared to other recent years.

Of the 255 arrests, 96 (38%) resulted in a charge, and 81% of these charges (relating to 78 individuals) were considered to be terrorism-related. Many of these cases are ongoing. Therefore, the number of charges resulting from the 255 arrests in the year ending 30 September 2016 can be expected to rise over time.

Of the 78 people charged with terrorism-related offences, 28 have been prosecuted and 48 are awaiting prosecution. 27 of the 28 prosecution cases led to individuals being convicted of an offence: 23 for terrorism-related offences and four for non-terrorism related offences.

As at 30 September 2016, there were 178 persons in custody in Great Britain² for terrorism-related offences and domestic extremism. This total was comprised of 169 persons in custody for terrorism-related offences and nine persons in custody for domestic extremism.

This was a decrease of eight persons compared to the situation as at 30 September 2015. This fall was driven by a reduction in the number of persons in custody for domestic extremism/separatism, which fell from 33 to nine over the same period. The number of individuals in custody for international terrorism has shown a steady increase in recent quarters.

Terrorism arrests and outcomes are often highly reliant on the investigatory powers and tools outlined in this report.

2 Data is provided to the Home Office by the National Offender Management Service and the Scottish Prison Service. As such, the statistics set out in this Chapter provide information on the number of persons in custody for terrorism-related offences and domestic extremism/separatism in Great Britain, not all areas of the United Kingdom.

Figure 1: Summary of key activity relating to those arrested in connection with terrorism-related offences in the year ending 30 September 2016

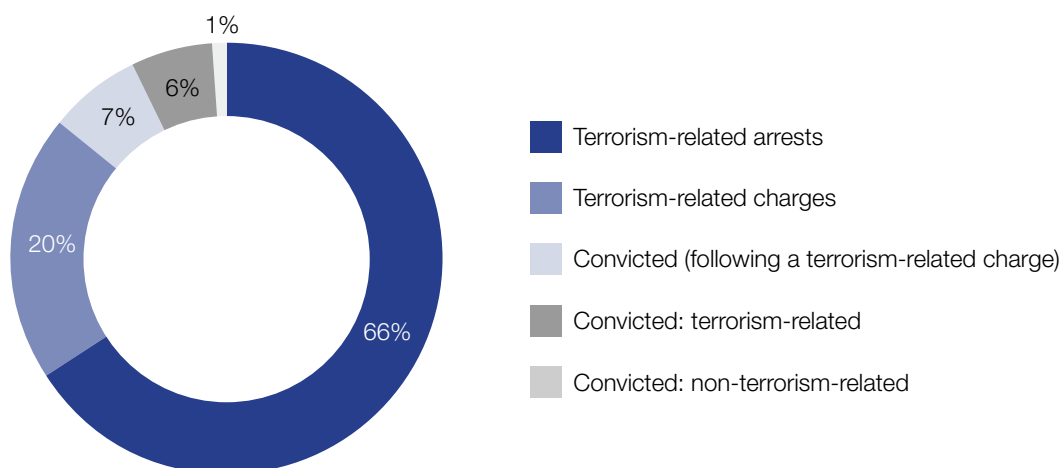
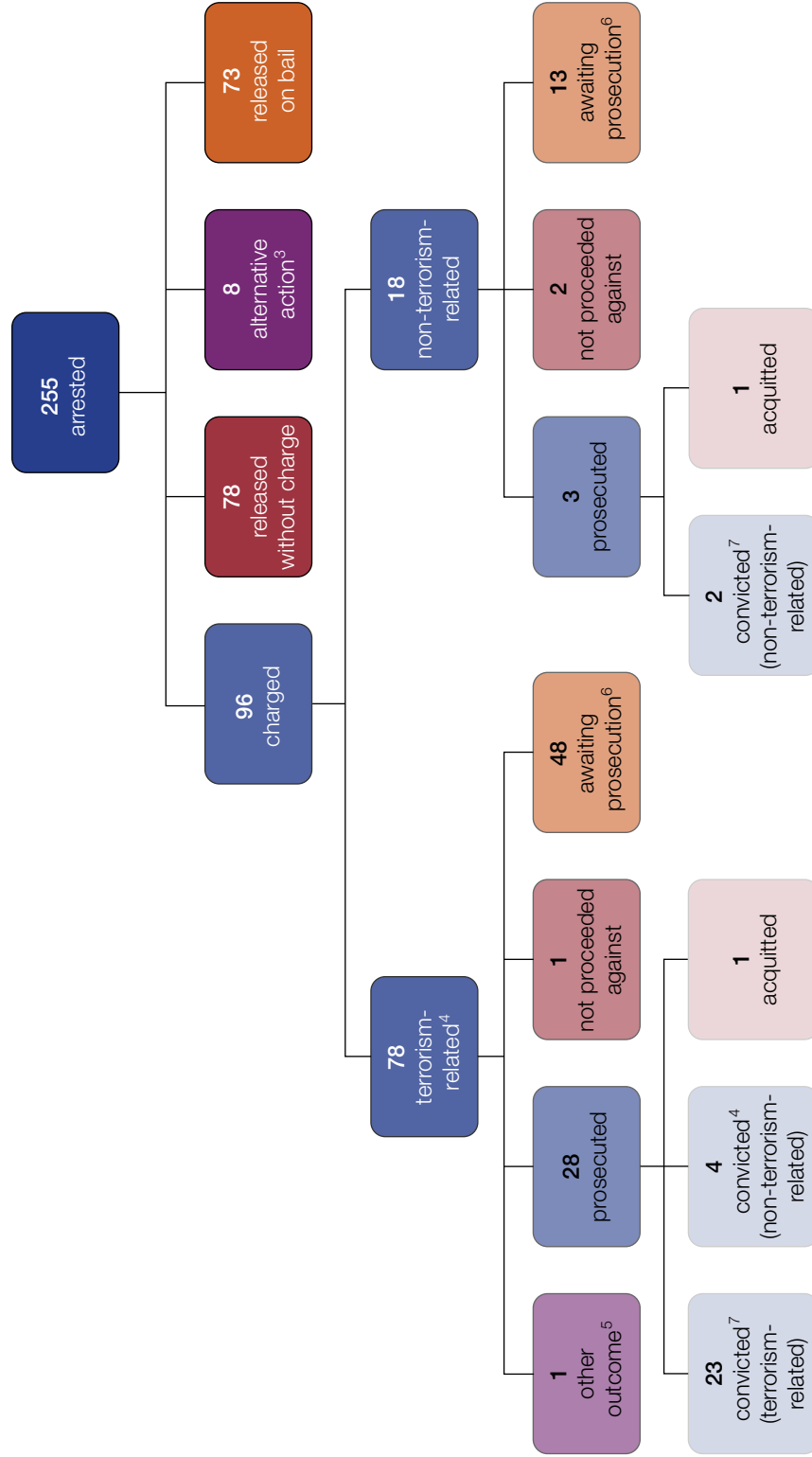


Figure 2: Arrests and outcomes,¹ year ending 30 September 2016²

The flow chart is designed to summarise how individuals who are arrested on suspicion of terrorism-related activity are dealt with throughout the criminal justice system. It follows the process from the point of arrest, through to charge (or other outcome) and prosecution.



Source: Home Office

Notes:

1. Based on time of arrest.
2. Data presented is based on the latest position with each case as at the date of data provision from National Counter-Terrorism Policing Functions Command (19 October 2016).
3. 'Alternative action' includes a number of outcomes, such as cautions, detentions under international arrest warrant, transfer to immigration authorities etc. See <https://www.gov.uk/government/statistics/operation-of-police-powers-under-the-terrorism-act-2000-quarterly-update-to-september-2016-data-tables> for a complete list.
4. Terrorism-related charges and convictions include some charges and convictions under non-terrorism legislation, where the offence is considered to be terrorism-related.
5. The 'other' category includes other cases/outcomes such as cautions, transfers to UK Border Agencies, the offender being circulated as wanted, and extraditions.
6. Cases that are 'awaiting prosecution' are not yet complete. As time passes, these cases will eventually lead to a prosecution, 'other' outcome, or it may be decided that the individual will not be proceeded against.
7. Excludes convictions that were later quashed on appeal.

4 – Serious Organised Crime Arrests and Outcomes

The National Crime Agency (NCA) is responsible for leading and coordinating the fight against serious and organised crime affecting the UK.

The NCA published its latest Annual Report and Accounts in July 2016.³ This report explained the NCA's response to the threat we face from serious and organised crime between 1 April 2015 and 31 March 2016. An outline of this activity is below.

It should be noted that these figures provide only an indication of the response to serious and organised crime. The NCA is focused on the disruptive impact of its activities against priority threats and high priority criminals and vulnerabilities, rather than merely on numbers of arrests or volumes of seizures. Furthermore, the UK's overall effort to tackle serious and organised crime also involves the work of a wide range of other public authorities, including police forces, Immigration Enforcement, Border Force and HM Revenue and Customs.

Arrests and Convictions

A significant part of the NCA's activity to disrupt serious and organised crime is to investigate those responsible in order that they can be prosecuted. In the period from 1 April 2015 to 31 March 2016, 1,763 individuals were arrested in the UK by NCA officers, or by law enforcement partners working on NCA-tasked operations and projects. In the same period, there were 915 convictions in relation to NCA casework and 1,329 disruptions. NCA activity also contributed to 1,300 arrests overseas.

Interdictions

Between 1 April 2015 and 31 March 2016, activity by the NCA resulted in the interdiction of 230 tonnes of drugs, including 120.8 tonnes of cannabis, 78.1 tonnes of cocaine, 3.5 tonnes of opium and 3.9 tonnes of heroin. In addition, during this period NCA activity resulted in the seizure of 323 guns and 16 other firearms.

3 "The National Crime Agency: Annual Report and Accounts 2015/2016" is available in full at www.nationalcrimeagency.gov.uk/publications

Criminal Finances

In the period from 1 April 2015 to 31 March 2016 the NCA recovered assets worth £26.9 million. In addition, the agency denied assets of £70.3 million. Asset denial activity included cash seizures, restrained assets and frozen assets.

Child Protection

In this reporting period, NCA activity led to 1,802 children being protected or safeguarded. Child protection is when action is taken to ensure the safety of a child, such as taking them out of a harmful environment. Child safeguarding is a broader term including working with children in their current environment, such as working with a school or referring a child for counselling.

As with terrorism arrests and convictions, serious and organised crime outcomes, such as those outlined above, are often highly reliant on the investigative powers outlined in this report.

5 – Disruptive Powers

It is not always possible to prosecute or deport terrorists and other individuals who threaten our national security. For example, where there is not enough evidence to advance a prosecution, or where there are concerns about an individual's treatment were they to be deported back to their country of origin.

It is therefore vital that the Government has the tools it needs to ensure the activities of individuals who pose a threat to our national security can be effectively disrupted.

This section of the report explains key disruptive powers the Government uses to keep the public safe, including details of their use and how this is limited by stringent safeguards.

5.1 – Stops and Searches

Powers of search and seizure are vital in ensuring that the police are able to acquire evidence in the course of a criminal investigation, and are powerful disruptive tools in the prevention of terrorism.

Section 47A of the Terrorism Act 2000 (TACT) enables a senior police officer to make an authorisation, specifying an area or place where they reasonably suspect that an act of terrorism will take place. Within that area and for the duration of the authorisation, a uniformed police constable may stop and search any vehicle or person for the purpose of discovering any evidence – whether or not they have a reasonable suspicion that such evidence exists – that the person is or has been concerned in the commission, preparation or instigation of acts of terrorism, or that the vehicle is being used for such purposes.

The authorisation must be necessary to prevent the act of terrorism which the authorising officer reasonably suspects will occur, and it must specify the minimum area and time period considered necessary to do so. The authorising officer must inform the Secretary of State of the authorisation as soon as is practicable, and the Secretary of State must confirm it. If the Secretary of State does not confirm the authorisation, it will expire 48 hours after being made. The Secretary of State may also substitute a shorter period, or a smaller geographical area, than was specified in the original authorisation.

Since it came into force no authorisations have been made in Great Britain under section 47A. This reflects the intention that the power should be reserved for exceptional circumstances, and the requirement that it only be used where necessary to prevent an act of terrorism that it is reasonably suspected is going to take place within a specified area and period. One authorisation has been made in Northern Ireland under section 47A, in unusual circumstances

which are described by the Independent Reviewer at paragraph 6.9 of his report on The Terrorism Acts in 2013. On 9 May 2013, the Court of Appeal held that the widely used stop and search powers under sections 21 and 24 of the Justice and Security (Northern Ireland) Act 2007 were not properly exercisable, since adequate safeguards to prevent their arbitrary use, in the form of a Code of Practice, were not in place. Considering that the statutory conditions for a section 47A authorisation were present, an Assistant Chief Constable of the PSNI issued an authorisation that day, covering parts of Northern Ireland. That authorisation was confirmed by the Secretary of State on 10 May 2013, and remained in place until a Code of Practice was introduced on 15 May 2013. 70 persons were stopped under the authorisation. The Independent Reviewer inspected the authorisation on a visit to Belfast in September 2013, at the request of the PSNI, and it was also inspected on another occasion by the Human Rights Advisor of the Northern Ireland Policing Board.⁴

Under sections 43 and 43A of TACT, police officers have further powers to stop and search, respectively, a person or vehicle. These powers do not require a section 47A authorisation to be in place. Instead they require the officer to reasonably suspect that the person is a terrorist or that the vehicle is being used for terrorist purposes.

In the year ending 30 June 2016, 552 persons were stopped and searched by the Metropolitan Police Service under section 43 of TACT (this data is not available in relation to other police forces). This represents a 26% increase from the previous year's total of 439. However, over the longer term, there has been a 55% fall in the number of stop and searches, from 1,229 in the year ending 31 March 2010 (the first year that figures are available for) to 552 in the year ending 30 June 2016. In the year ending 30 June 2016, the arrest rate of those stopped and searched under section 43 was 12%, up from 8% in the previous year.⁵

5.2 – Port and Border Controls

Schedule 7 to the Terrorism Act 2000 (Schedule 7) helps protect the public by allowing an examining police officer to stop and question and, when necessary, detain and search individuals travelling through ports, airports, international rail stations or the border area. The purpose of the questioning is to determine whether that person appears to be someone who is, or has been, involved in the commission, preparation or instigation of acts of terrorism. The Schedule 7 power also extends to examining goods to determine whether they have been used in the commission, preparation or instigation of acts of terrorism.

Prior knowledge or suspicion that someone is involved in terrorism is not required for the exercise of the Schedule 7 power. Examinations are also about talking to people in respect of whom there is no suspicion but who, for example, are travelling to and from places where terrorist activity is taking place or emerging, to determine whether those individuals are, or have been, involved in terrorism. This is particularly important given the current threat from Syria and Iraq.

⁴ Further details may be found at <https://terrorismlegislationreviewer.independent.gov.uk>

⁵ Full statistical releases on the operation of police powers under the Terrorism Act 2000, including stop and search powers, are available at www.gov.uk/government/collections/counter-terrorism-statistics

The Schedule 7 Code of Practice for examining officers provides guidance on the selection of individuals for examination. The most recent version of the Code came into effect on 25 March 2015.⁶ Selection for questioning under Schedule 7 is based on the current terrorist threat to the UK posed by the various terrorist groups active in and outside the UK. Selection is made on the basis of informed considerations. This can include intelligence, which may be imprecise and relate to events and places rather than to specific people. Requiring suspicion of individuals would severely curtail the ability of the police to examine people to determine their involvement in terrorism.

When an individual is examined under Schedule 7 they are given a Public Information Leaflet. The Public Information Leaflet is available in multiple languages and outlines the purpose and provisions of Schedule 7, obligations under Schedule 7, key points of the Code of Practice including an individual's rights and relevant contact details (including those needed to provide feedback or make a complaint). An individual can be examined for more than an hour only if that person is formally detained. This requirement ensures examinees' rights are safeguarded; the statutory review of detention process begins after one hour, and detainees have the right to legal advice for examinations which take longer than one hour.

An individual can complain about a Schedule 7 examination by writing to the Chief Officer of the police force for the area in which the examination took place. Additionally, the Independent Reviewer of Terrorism Legislation is responsible for reporting each year on the operation of the Schedule 7 power.

Statistics on the operation of Schedule 7 powers are published by the Home Office on a quarterly basis.⁷ In the year ending 30 June 2016, a total of 23,717 persons were examined under this power in Great Britain, a fall of 23% on the previous year. Throughout the same period, the number of detentions following examinations increased by 7% from 1,649 in the year ending 30 June 2015 to 1,760 in the year ending 30 June 2016.

Of those individuals that were detained (excluding those who did not state their ethnicity), 41% categorised themselves as 'Asian or Asian British'. The next most predominant ethnic groups were 'Chinese or Other' at 29% and 'White' at 14%. The proportion of those that categorised their ethnicity as 'Black or Black British' or 'Mixed' made up 9% and 7% respectively.

Certain travel routes are given greater focus, given that the use of Schedule 7 is based on the current terrorist threat to the UK and the intelligence underpinning the threat assessment. Self-defined members of ethnic minority communities do comprise a majority of those examined under Schedule 7. However, the proportion of those examined should correlate not to the ethnic breakdown of the general population, or even the travelling population, but to the ethnic breakdown of the terrorist population. In successive reports the Independent Reviewer of Terrorism Legislation, David Anderson QC, has confirmed that he has no reason to believe

6 The full Schedule 7 Code of Practice is available at <https://www.gov.uk/government/publications/code-of-practice-for-examining-officers-and-review-officers-under-schedule-7-to-the-terrorism-act-2000>

7 Full statistical releases on the operation of police powers under the Terrorism Act 2000 are available at www.gov.uk/government/collections/counter-terrorism-statistics

that Schedule 7 powers are exercised in a racially discriminatory way. This assessment was endorsed in 2015 by the Supreme Court in their comments in the case of *Beghal*. In the year ending June 2016, 23,717 people were stopped under Schedule 7 power in Great Britain.⁸ In the same period, approximately 250 million people travelled through UK ports.

Since April 2015, the Home Office has collected data relating to the use of these powers. This data includes the number of goods examinations (sea and air freight), the number strip searches conducted, and the number of refusals following a request by an individual to postpone questioning. In the year ending 30 June 2016, a total of 3,855 air freight and 6,390 sea freight examinations were conducted in Great Britain. Regarding strip searches, there were seven instances carried out under Schedule 7. Postponement of questioning (usually to enable an individual to consult a solicitor) was refused three times.

5.3 – Terrorist Asset-Freezing

The UK terrorist asset-freezing regime is an important disruptive tool, which aims to stop terrorist acts by preventing funds, economic resources or financial services from being made available to, or used by, someone who might use them for terrorist purposes. The power can be exercised in cases where a criminal prosecution is not possible, and to prevent assets being dissipated when suspects are arrested, provided the relevant statutory test is met.

The UK asset-freezing regime meets obligations placed on the UK by Resolutions of the UN Security Council and associated European Commission Regulations. Meeting these obligations is, in turn, also part of the global standards set by the Financial Action Task Force (FATF). FATF will evaluate the UK's compliance with its standards in 2018. The UK terrorist asset-freezing regime is implemented by the Terrorist Asset-Freezing etc. Act 2010 (TAFE).⁹

TAFE gives the Treasury the power to impose financial restrictions on individuals and groups believed to be involved in terrorist activity, whether in the UK or abroad. These restrictions have the effect of freezing any funds or assets in the UK belonging to the designated person or entity. They also make it an offence for any person to make funds, financial services or economic resources available to, or available for the benefit of, a designated person or entity where that person knows, or has reasonable cause to suspect, the individual or entity is designated. The Treasury does not proactively identify targets for asset freezes. Rather, the Treasury is advised by operational partners, including the police and Security Service, who identify possible targets for asset freezes and present the evidence supporting the freeze to the Treasury to consider. It is also possible for third countries to identify possible targets, although this is less common.

The UK's terrorist asset-freezing regime contains robust safeguards to ensure the restrictions remain proportionate. Under section 2(1)(a) of TAFE, the Treasury may only designate persons

⁸ Home Office statistical bulletin (September 2016), Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search, Great Britain, quarterly update to June 2016. Available online at: <https://www.gov.uk/government/statistics/operation-of-police-powers-under-the-terrorism-act-2000-quarterly-update-to-june-2016>

⁹ The Terrorist Asset-Freezing etc Act 2010 is available at www.legislation.gov.uk/ukpga/2010/38/contents

where it has reasonable grounds to believe that they are, or have been, involved in terrorist activity, or are owned, controlled or acting on behalf of someone who is, or has been, involved in terrorist activity. Under section 2(1)(b), a designation may only be made where the Treasury considers it necessary for purposes connected with protecting members of the public (anywhere in the world) from terrorism. The requirements of both section 2(1)(a) and 2(1)(b) must be met for a designation to be made.

In addition, there are a number of other safeguards to ensure that the UK's terrorist asset-freezing regime is operated fairly and proportionately:

- The Treasury may grant licences to allow exceptions to the freeze, ensuring that human rights are taken account of, whilst also ensuring that funds are not diverted to terrorist purposes;
- Designations expire after a year unless reviewed and renewed. The Treasury may only renew a designation where the requirements under sections 2(1)(a) and (b) of TAFE continue to be met;
- Designations must generally be publicised but can be notified on a restricted basis and not publicised when one of the conditions in section 3 of TAFE is met. Conditions are that either: the individual is under 18; or it is in the interests of national security or justice for only certain people to be informed of the designation; or for reasons connected with the prevention or detection of serious crime;
- Where a designation is notified on a restricted basis, the Treasury can also specify that people informed of the designation treat the information as confidential;
- A designated person (or entity) has a right of appeal against a designation decision in the High Court, and anyone affected by a licensing decision (including the designated person (or entity)) can challenge on judicial review grounds any licensing or other decisions of the Treasury under TAFE. There is a closed material procedure available for such appeals or challenges using specially cleared advocates to protect closed material whilst ensuring a fair hearing for the affected person;
- Individuals are notified, as far as it is in the public interest to do so, of the reasons for their designation. This information is kept under review and if it becomes possible to release more detailed reasons the Treasury will do so;
- The Independent Reviewer of Terrorism Legislation, David Anderson QC, may conduct a review of, and report on, the operation of the TAFE;¹⁰ and
- The Treasury is required to report to Parliament, quarterly, on its operation of the UK's asset freezing regime. In addition, the Treasury also reports on the UK's operation of the EU and UN terrorist asset-freezing regimes.

10 David Anderson's latest annual report on the operation of the Terrorist Asset-Freezing etc. Act 2010 (TAFE) is available at <https://terrorismlegislationreviewer.independent.gov.uk/category/reports/>

In addition to the UK's domestic terrorist asset-freezing regime under TAFE, the Government is also responsible for the UK's operation of other counter-terrorism asset-freezing regimes:

- The UN ISIL (Daesh) and Al-Qaida regime takes direct effect in the UK through Council Regulation (EC) 881/2002. UN ISIL (Daesh) and Al-Qaida asset freezes are approved by Security Council members and are listed by the UN. These freezes apply in all UN Member States and a travel ban is also applied. Under this asset-freezing regime, the Treasury has responsibility for licensing and compliance in the UK under the *ISIL (Daesh) and Al-Qaida (Asset-Freezing) Regulations 2011*. Following the EU's implementation, in March 2016, of the changes the UN made to the regime in December 2015, the Government amended the *Al-Qaida (Asset-Freezing) Regulations 2011* in September 2016, reflecting these changes, including the amended regime name, in the relevant UK Statutory Instrument.
- The EU ISIL (Daesh) and Al-Qaida regime. The Council of the European Union on 20 September adopted Council Regulation (EU) 2016/1686, giving the EU autonomous power to impose restrictive measures including asset freezes, on Al-Qaida and ISIL individuals and entities. These restrictive measures apply in all EU member states. As with the UN regime, the Treasury has responsibility for licensing and compliance with the regime in the UK under the *ISIL (Daesh) and Al-Qaida (Asset-Freezing) Regulations 2011*.
- The EU CP931 regime. Under EU Common Position 931 (CP931), such asset freezes can only be applied to persons who are not associated with Al-Qaida or ISIL (Daesh), who are external to the EU, and in relation to whom another Member State has made a prior competent authority decision to impose restrictive measures. Home-grown terrorists not linked to groups outside the EU cannot have their assets frozen under this regime. Under this regime, the EU has responsibility for designations and the Treasury has responsibility for licensing and compliance with the regime in the UK under Part 1 of TAFE. UK operation of this regime takes place under Council Regulation (EC) 2580/2001.

The most recent quarterly publication by the Treasury on the operation of the UK's asset-freezing regime covers the period 1 July 2016 to 30 September 2016. Under TAFE, as at 30 September 2016, there were £9,000 of assets frozen, covering six accounts in the UK. At the end of the reporting period, there were a total of 21 extant designations. There were no new designations during this reporting period.

In addition, as at 30 September 2016, under the EU asset-freezing regime, there was one empty frozen account. This figure does not duplicate funds frozen under TAFE. Under the EU regime, no new accounts were frozen or unfrozen during this reporting period.

Under the UN asset-freezing regime, there was £66,000 of assets frozen as at 30 September 2016, across 34 accounts. No new accounts were frozen during this reporting period and no accounts were unfrozen.

Other key figures from this reporting period are at **ANNEX A**.¹¹

¹¹ Full statistical reports for this and previous periods can be found at www.gov.uk/government/collections/operation-of-the-uks-counter-terrorist-asset-freezing-regime-quarterly-report-to-parliament

5.4 – Terrorism Prevention and Investigation Measures

Terrorism Prevention and Investigation Measures (TPIMs) allow the Home Secretary to impose a powerful range of disruptive measures on a small number of people who pose a threat to our security but who cannot be prosecuted or, in the case of foreign nationals, deported. These measures can include: overnight residence requirements, including relocation to another part of the UK; daily police reporting; wearing an electronic monitoring tag; exclusion from specific places; limits on association; limits on the use of financial services and the use of telephones and computers; and a ban on holding travel documents.

It is the Government’s assessment that, for the foreseeable future, there will remain a small number of individuals who pose a threat to our security but who cannot be either prosecuted or deported. We are clear that there continues to be a need for powers to protect the public from the threat these people pose. This is why we need TPIMs.

The use of TPIMs is subject to stringent safeguards. Before deciding to impose a TPIM notice on an individual, the Secretary of State must be satisfied that five conditions are met, as set out at section 3 of the Terrorism Prevention and Investigation Measures Act 2011 (TPIM Act).¹² The conditions are that:

- the Secretary of State considers, on the balance of probabilities, that the individual is, or has been, involved in terrorism-related activity (the “relevant activity”);
- some or all of the relevant activity is new terrorism-related activity;
- the Secretary of State reasonably considers that it is necessary, for purposes connected with protecting members of the public from a risk of terrorism, for Terrorism Prevention and Investigation Measures to be imposed on the individual;
- the Secretary of State reasonably considers that it is necessary, for purposes connected with preventing or restricting the individual’s involvement in terrorism-related activity, for the specified Terrorism Prevention and Investigation Measures to be imposed on the individual; and
- the court gives permission, or the Secretary of State reasonably considers that the urgency of the case requires Terrorism Prevention and Investigation Measures to be imposed without obtaining such permission.

The Secretary of State must apply to the High Court for permission to impose the TPIM notice on the individual, except in urgent cases where the notice must be immediately referred to the court for confirmation.

All individuals upon whom a TPIM notice is imposed are automatically entitled to a review hearing at the High Court relating to the decision to impose the notice and the individual measures in the notice. They may also appeal against any decisions made subsequent to the imposition of the notice i.e. a refusal of a request to vary a measure, a variation of a measure

¹² The Terrorism Prevention and Investigation Measures Act 2011 is available at www.legislation.gov.uk/ukpga/2011/23

without their consent, or the revival or extension of their TPIM notice. The Secretary of State must keep under review the necessity of the TPIM notice and specified measures during the period that a TPIM notice is in force.

A TPIM notice initially lasts for one year and can only be extended for one further year. No new TPIM may be imposed on the individual after that time unless the Secretary of State considers on the balance of probabilities that the individual has engaged in further terrorism-related activity since the imposition of the notice.

In recognition of the severity of the threats we face, the Counter-Terrorism and Security Act 2015 enhanced the powers available in the TPIM Act, including introducing the ability to relocate a TPIM subject elsewhere in the UK (up to a maximum of 200 miles from their normal residence), and a power to require a subject to attend meetings as part of their ongoing management, such as with the probation service or Jobcentre Plus staff. In 2015, the Home Office also published factors which the then Home Secretary, the Rt. Hon. Theresa May MP, considered appropriate to take into account when considering whether to relocate a subject under the overnight residence measure.¹³ These are: the need to prevent or restrict a TPIM subject's involvement in terrorism-related activity; the personal circumstances of the individual; proximity to travel links including public transport, airports, ports and international rail terminals; the availability of services and amenities, including access to employment, education, places of worship and medical facilities; proximity to prohibited associates; proximity to positive personal influences; location of UK resident family members; and community demographics.

The Independent Reviewer of Terrorism Legislation, David Anderson QC, has a statutory duty to review the Terrorism Prevention and Investigation Measures Act 2011. He has, to date, published an annual report setting out an assessment of the use of the power and any recommendations to improve its use, though changes made to the Independent Reviewer's remit through the Counter-Terrorism and Security Act 2015 allow for a more flexible arrangement in respect of the frequency of this review.¹⁴

Under the TPIM Act, the Secretary of State is required to report to Parliament, as soon as reasonably practicable after the end of every relevant three month period, on the exercise of TPIM powers.

The most recent report covers the period from 1 September 2016 to 30 November 2016. As at 30 November 2016, there were seven TPIM notices in force, six of which related to a British citizen. There were no extensions, revocations or revivals of TPIM notices between 1 September 2016 and 30 November 2016. There were four variations made to measures specified in TPIM notices during the reporting period and one application to vary a measure refused. As of 30 November 2016, seven TPIM subjects have been relocated under TPIM legislation.¹⁵

13 Written Ministerial Statement on Terrorism and Prevention Measures, laid on 12 February 2015.

14 David Anderson's latest annual report on the operation of TPIMs is available at <https://terrorismlegislationreviewer.independent.gov.uk/category/reports/tpims-control-orders/>

15 The latest quarterly report on the exercise of TPIMs is available in full at www.parliament.uk

5.5 – Royal Prerogative

The Royal Prerogative is an important tool used to disrupt individuals who seek to travel abroad on a British passport to engage in terrorism-related activity and who would return to the UK with enhanced capabilities to do the public harm.

A passport, whether valid or cancelled, remains the property of the Crown. HM Passport Office issues passports under the Royal Prerogative and there are a number of grounds for withdrawal or refusal. The Home Secretary has the discretion, under the Royal Prerogative, to refuse to issue or to cancel a British passport on public interest grounds. This criteria supports the use of the Royal Prerogative in national security cases. Secretaries of State exercise a range of prerogative powers in different contexts and the courts have upheld the legitimacy of prerogative powers that are not based in primary legislation.

Using the Royal Prerogative, persons may be refused a British passport or may have their existing passport withdrawn on a number of grounds, including that the grant to them, or their continued enjoyment of passport facilities is contrary to the public interest. Public interest grounds include seeking to harm the UK or its allies by travelling on a British passport to, for example, engage in terrorism-related activity.

On 25 April 2013, the Government redefined the public interest criteria to refuse or withdraw a passport in a Written Ministerial Statement to Parliament. The policy allows passports to be withdrawn, or refused, where the Home Secretary is satisfied that it is in the public interest to do so. This may be the case for:

“A person whose past, present or proposed activities, actual or suspected, are believed by the Home Secretary to be so undesirable that the grant or continued enjoyment of passport facilities is contrary to the public interest.”¹⁶

There may be circumstances in which the application of legislative powers is not appropriate to an individual, but there is a need to restrict the ability of a person to travel abroad.

The application of discretion by the Home Secretary will primarily focus on preventing overseas travel. There may be cases in which the Home Secretary believes that the past, present or proposed activities (actual or suspected) of the person applying for a passport, or passport holder should prevent their enjoyment of a passport facility whether overseas travel is or is not a critical factor.

Following the Secretary of State’s statement in April 2013, the Royal Prerogative was used six times in 2013, 24 times in 2014 and 23 times in 2015 in relation to national security. These figures refer to occasions where an individual’s passport was either revoked or their application for a passport was refused on public interest grounds.

¹⁶ The full Written Ministerial Statement is available at www.gov.uk/government/speeches/the-issuing-withdrawal-or-refusal-of-passports

5.6 – Seizure and Temporary Retention of Travel Documents

Schedule 1 to the Counter-Terrorism and Security Act 2015 enables police officers at ports to seize and temporarily retain travel documents to disrupt immediate travel, when they reasonably suspect that a person intends to travel to engage in terrorism related activity outside the UK.

The temporary seizure of travel documents provides the authorities with time to investigate an individual further, and consider taking longer term disruptive action, such as prosecution, exercising the Royal Prerogative to cancel or refuse to issue a British passport, or making a person subject to a TPIM order.

Travel documents can only be retained for up to 14 days while investigations take place. The police may apply to the courts to extend the retention period, but this must not exceed 30 days in total.

Between February and December 2015, the power was exercised 24 times and in some cases has led to longer-term disruptive action such as using the Royal Prerogative power to cancel a British passport.

5.7 – Exclusions

The Secretary of State (usually the Home Secretary) may decide to exclude a foreign national if he or she considers that the person's presence in the UK would not be conducive to the public good, if a decision to exclude would be reasonable, consistent and proportionate based on the evidence available. The exclusion power arises under the Royal Prerogative. It is normally used in circumstances involving national security, unacceptable behaviour (such as extremism), international relations or foreign policy, and serious and organised crime.

European Economic Area nationals and their family members may be excluded from the UK on grounds of public policy or public security, if they are considered to pose a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society.

Between 11 May 2010 and 31 December 2015, the Government excluded 181 people from the United Kingdom, including 69 exclusions on national security grounds. There were 26 exclusions made between 1 January 2015 and 31 December 2015.

The Secretary of State will use exclusion powers when justified and based on all available evidence. In all matters, the Secretary of State must act reasonably, proportionately and consistently. Exclusion powers are very serious and the Government does not use them lightly.

5.8 – Temporary Exclusion Orders

The Counter Terrorism and Security Act 2015 introduced Temporary Exclusion Orders (TEOs). This is a statutory power which allows the Secretary of State (usually the Home Secretary) to disrupt and control the return to the UK of a British citizen who has been involved in terrorism-related activity outside the UK.

The policy was developed in line with the UK's international legal obligations including the European Convention on Human Rights, the UN Convention on the Reduction of Statelessness, and the EU Free Movement Directive.

A TEO makes it unlawful for the subject to return to the UK without engaging with the UK authorities. It is implemented through cancelling the TEO subject's travel documents and adding them to watch lists (including the authority-to-carry 'no fly' list), ensuring that when individuals do return, it is in a manner which the UK Government controls. The subject of a TEO commits an offence if, without reasonable excuse, he or she re-enters the UK not in accordance with the terms of the order.

A TEO also allows for certain obligations to be imposed once the individual returns to the UK and during the validity of the order. These might include reporting to a police station, notifying the police of any change of address, or attending appointments such as a de-radicalisation programme. The subject of a TEO also commits an offence if, without reasonable excuse, he or she breaches any of the conditions imposed.

There are two stages of judicial oversight for TEOs. The first is a court permission stage before a TEO is imposed by the Secretary of State. The second is a statutory review of the decision to impose a TEO and any in-country obligations after the individual has returned to the UK.

Since the power came into force in the second quarter of 2015, it has not been used.

5.9 – Deprivation of British Citizenship

The British Nationality Act 1981 provides the Secretary of State with the power to deprive an individual of their British citizenship in certain circumstances. Such action paves the way for possible immigration detention, deportation or exclusion from the UK.

The Secretary of State may deprive an individual of their British citizenship if satisfied that such action is 'conducive to the public good' or if the individual obtained their British citizenship by means of fraud, false representation or concealment of material fact.

When seeking to deprive a person of their British citizenship on the basis that to do so is 'conducive to the public good', the law requires that this action only proceeds if the individual concerned would not be left stateless (no such requirement exists in cases where the citizenship was obtained fraudulently).

The Government considers that deprivation on ‘conducive’ grounds is an appropriate response to activities such as those involving:

- national security, including espionage and acts of terrorism directed at this country or an allied power;
- unacceptable behaviour of the kind mentioned in the then Home Secretary’s statement of 24 August 2005 (‘glorification’ of terrorism etc);
- war crimes; and
- serious and organised crime.

By means of the Immigration Act 2014, the Government introduced a power whereby in a small subset of ‘conducive’ cases – where the individual has been naturalised as a British citizen and acted in a manner seriously prejudicial to the vital interests of the UK – the Secretary of State may deprive that person of their British citizenship, even if doing so would leave them stateless. This action may only be taken if the Secretary of State has reasonable grounds for believing that the person is able, under the law of a country outside the United Kingdom, to become a national of that country.

In practice, this power means the Secretary of State may deprive and leave a person stateless (if the vital interest test is met and they are British due to naturalising as such), if that person is able to acquire (or reacquire) the citizenship of another country and is able to avoid remaining stateless.

The Immigration Act 2014 also required this additional element of the deprivation power to be reviewed after the first year of being in force (and at three-year intervals thereafter). Therefore in July 2015, David Anderson QC, the Independent Reviewer of Terrorism Legislation, accepted an invitation from the then Immigration Minister to carry out the statutory review. The review covered the period 30 July 2014 to 29 July 2015 and was published on 21 April 2016.¹⁷

The Government considers removal of citizenship to be a serious step, one that is not taken lightly. This is reflected by the fact that the Home Secretary personally decides whether such action should be taken, where it is considered that it may be conducive to the public good to deprive an individual of citizenship.

Between 1 January 2015 and 31 December 2015, five people were deprived of British citizenship on the basis that to do so was conducive to the public good.¹⁸

5.10 – Deportation with Assurances

Where prosecution is not possible, the deportation of foreign nationals to their country of origin may be an effective alternative means of disrupting terrorism-related activities. Where

¹⁷ A copy of the Independent Reviewer’s subsequent report can be found at <https://www.gov.uk/government/publications/citizenship-removal-resulting-in-statelessness>

¹⁸ Figures derived from internal Home Office information.

there are concerns for an individual’s safety on return, government-to-government assurances may be used to achieve deportation in accordance with the UK’s human rights obligations.

Deportation with Assurances (DWA) enables the UK to reduce the threat from terrorism by deporting foreign nationals who pose a risk to our national security, while still meeting our domestic and international human rights obligations, including Article 3 of the European Convention on Human Rights, which prohibits torture and inhuman or degrading treatment or punishment.

Assurances in individual cases are the result of careful and detailed discussions, endorsed at a very high level of government, with countries with which we have working bilateral relationships. We may also put in place arrangements – often including monitoring by a local human rights body – to ensure that the assurances can be independently verified. The use of DWA has been consistently upheld by the domestic and European courts.

We have also asked the Independent Reviewer of Terrorism Legislation, David Anderson QC, to review the legal framework of DWA to examine whether the process can be improved, including by learning from the experiences of other countries.

A total of 12 people have been removed from the UK under DWA arrangements.¹⁹

5.11 – Proscription

Proscription is an important tool enabling the prosecution of individuals who are members or supporters of, or are affiliated with, a terrorist organisation. It can also support other disruptive powers including prosecution for wider offences, immigration powers such as exclusion, and terrorist asset freezing. The resources of a proscribed organisation are terrorist property and are, therefore, liable to be seized.

Under the Terrorism Act 2000, the Home Secretary may proscribe an organisation if she believes it is concerned in terrorism. For the purposes of the Act, this means that the organisation:

- commits or participates in acts of terrorism;
- prepares for terrorism;
- promotes or encourages terrorism (including the unlawful glorification of terrorism); or
- is otherwise concerned in terrorism.

“Terrorism” as defined in the Act, means the use or threat of action which: involves serious violence against a person; involves serious damage to property; endangers a person’s life (other than that of the person committing the act); creates a serious risk to the health or safety of the public or section of the public; or is designed seriously to interfere with or seriously to disrupt an electronic system. The use or threat of such action must be designed to influence the government or an international governmental organisation or to intimidate the public or

¹⁹ Figures derived from internal Home Office information.

a section of the public and be undertaken for the purpose of advancing a political, religious, racial or ideological cause.

If the statutory test is met, there are other factors which the Secretary of State will take into account when deciding whether or not to exercise the discretion to proscribe. These discretionary factors are:

- the nature and scale of an organisation's activities;
- the specific threat that it poses to the UK;
- the specific threat that it poses to British nationals overseas;
- the extent of the organisation's presence in the UK; and
- the need to support other members of the international community in the global fight against terrorism.

Proscription under the Terrorism Act 2000 makes it a criminal offence to:

- belong, or profess to belong, to a proscribed organisation (section 11 of the Act);
- invite support for a proscribed organisation (and the support is not, or is not restricted to the provision of money or other property) (section 12 (1));
- arrange, manage or assist in arranging or managing a meeting in the knowledge that the meeting is to support or further the activities of a proscribed organisation, or is to be addressed by a person who belongs or professes to belong to a proscribed organisation (section 12 (2)); or to address a meeting if the purpose of the address is to encourage support for, or further the activities of, a proscribed organisation (section 12 (3)); and
- wear clothing or carry or display articles in public in such a way or in such circumstances as arouse reasonable suspicion that an individual is a member or supporter of the proscribed organisation (section 13).

The penalties for proscription offences under sections 11 and 12 are a maximum of 10 years in prison and/or a fine. The maximum penalty for a section 13 offence is six months in prison and/or a fine not exceeding £10,000.

Under the Terrorism Act 2000, a proscribed organisation, or any other person affected by a proscription, may submit a written application to the Home Secretary, asking that a consideration be made whether a specified organisation should be removed from the list of proscribed organisations. The application must set out the grounds on which it is made. The precise requirements for an application are contained in the Proscribed Organisations (Applications for Deproscription etc) Regulations 2006 (SI 2006/2299).

The Home Secretary is required to determine the application within 90 days from the day after it is received. If the deproscription application is refused, the applicant may make an appeal to the Proscribed Organisations Appeals Commission (POAC). The Commission will allow an appeal if it considers that the decision to refuse deproscription was flawed, applying

judicial review principles. Either party can seek leave to appeal the POAC's decision at the Court of Appeal.

If the Home Secretary agrees to deproscribe the organisation, or the appeal is allowed, the Home Secretary will lay a draft order before Parliament removing the organisation from the list of proscribed organisations. The Order is subject to the affirmative resolution procedure so must be agreed by both Houses of Parliament.

The Mujaheddin e Khalq (MeK) also known as the Peoples' Mujaheddin of Iran (PMOI) was removed from the list of proscribed groups in June 2008 as a result of judgments of the POAC and the Court of Appeal.

The International Sikh Youth Federation (ISYF) was removed from the list of proscribed groups in March 2016 following receipt of an application to deproscribe the organisation.

There are currently 71²⁰ international terrorist organisations proscribed under the Terrorism Act 2000. In addition, there are 14 organisations in Northern Ireland that were proscribed under previous legislation. In December 2016, National Action became the first extreme right-wing group to be proscribed following its move from extremism into terrorism.

Information about these groups' aims was given to Parliament at the time that they were proscribed. These details, for each proscribed international terrorist organisation, are included at **ANNEX B**.

5.12 – Closed Material Procedure

The Justice and Security Act 2013 introduced a new statutory closed material procedure (CMP), which allows for sensitive material which would be damaging to national security to be examined in civil court proceedings.²¹ CMPs ensure that, Government Departments, the Security and Intelligence Agencies, law enforcement and indeed any other party to proceedings have the opportunity to properly defend themselves, or bring proceedings, in the civil court, where sensitive national security material is considered by the court to be involved. CMPs allow the courts to scrutinise matters that were previously not heard because disclosing the relevant material publicly would have damaged national security.

A declaration permitting closed material applications is an "in principle" decision made by the court about whether a CMP should be available in the relevant case. This decision is normally based on an application from a party to the proceedings, usually a Secretary of State. However, the court can also make a declaration of its own motion.

Where a Secretary of State makes the application, the court must first satisfy itself that the Secretary of State has considered making, or advising another person to make an application for public interest immunity in relation to the material. The court must also be satisfied that

20 The actual number of proscribed organisations is lower than this figure as some groups appear on the list of proscribed organisations under more than one name, for example, 'Al Ghurabaa' and 'The Saved Sect' both refer to the group commonly known as 'Al Muhajiroun'.

21 The Justice and Security Act is available at www.legislation.gov.uk/ukpga/2013/18/contents

material would otherwise have to be disclosed which would damage national security, and that closed proceedings would be in the interest of the fair and effective administration of justice. Should the court be satisfied that the above criteria are met, then a declaration may be made. During this part of proceedings a Special Advocate may be appointed to act in the interests of parties excluded from proceedings.

Once a declaration is made, the Act requires that the decision to proceed with a CMP is kept under review and, if necessary, the CMP may be revoked by a judge at any stage of proceedings.

A further hearing, following a declaration, determines which parts of the case should be dealt with in closed proceedings and which should be released into open proceedings. The test being considered here remains whether the disclosure of such material would damage national security.

The Justice and Security Act requires the Secretary of State to prepare (and lay before Parliament) a report on CMP applications and subsequent proceedings under section 6 of the Act. Under section 12(4) of the Act, the report must be prepared and laid before Parliament as soon as reasonably practicable after the end of the 12 month period to which the report relates. The first report covered the period 25 June 2013 (when the Act came into force) to 24 June 2014.²² The most recent report, relating to the period 25 June 2015 to 24 June 2016, was published on 16 November 2016.²³

In the latest reporting period from 2015 to 2016, there were 12 applications for a declaration that a CMP application may be made (eight of them by the Secretary of State, and four by persons other than the Secretary of State). There were seven declarations that a CMP application may be made in proceedings during the reporting period (three in response to applications made by the Secretary of State during the reporting period, and four in response to applications made by the Secretary of State during previous reporting periods). None of the declarations were revoked.

There were six final judgements during this period (all of them were not closed judgements, made regarding the outcome of the application for a CMP).

5.13 – Tackling Online Extremism

The internet is a powerful tool which terrorists and extremists exploit to spread hate, radicalise, recruit, inspire and incite. Terrorist groups like Daesh make extensive use of the internet to spread their messages through a growing social media presence and compelling propaganda designed to reach a wider audience. This can be a contributory factor in an individual's radicalisation process, tipping them into condoning or undertaking violent acts.

²² <https://www.gov.uk/government/publications/report-on-use-of-closed-material-procedure-june-2013-to-june-2014>

²³ <https://www.gov.uk/government/collections/use-of-closed-material-procedure-reports>

We are taking robust action to take down terrorist and extremist material and to support those who are challenging them online. We are also working to help people resist extremists' poisonous ideology.

Our dedicated police Counter Terrorism Internet Referral Unit (CTIRU) refers content that they assess as contravening UK terrorism legislation to communications service providers (CSPs). If CSPs agree that it breaches their terms and conditions, they remove the content voluntarily. CTIRU does not remove content itself. Since its inception in February 2010, CTIRU has secured the removal of more than 220,000 pieces of terrorist-related content. The Europol Internet Referrals Unit (EUIRU) replicates this model at European level and services all Member States.

Industry cooperation has continuously improved since the CTIRU was established, leading to faster and more consistent removal of content. CTIRU has established relationships with over 300 CSPs of differing sizes. Removals at the request of CTIRU have increased from around 60 items a month in 2010, when CTIRU was first established, to over 6000 a month in 2015. These arrangements mean that where companies take action, this removes access to the content from the whole platform, not just for users accessing it from within a particular jurisdiction, and therefore has a world-wide benefit.

Going forward, our aim is to encourage industry to lead and take a proactive approach in tackling terrorist and extremist abuse of their platforms. Overall, we wish to see a swifter, more comprehensive approach to removing content.

Alongside our effort to squeeze the space terrorists and extremists operate online, we work with a range of civil society groups to counter extremist ideologies and to equip people in communities with the ability to reject those narratives.

5.14 – Tackling Online Child Sexual Exploitation

The Government is undertaking a significant programme of work to enhance the UK's response to online child sexual exploitation (CSE).

In February 2015, the Director General of the National Crime Agency (NCA) used his powers under the Crime and Courts Act to task National Police Chiefs' Council (NPCC) to produce a plan to tackle online CSE. Collaborative working between police forces and the NCA against this plan is resulting in around 375 arrests each month for online CSE offences, and the safeguarding of around 450 children each month.

The WeProtect Summit, which took place on 10 and 11 December 2014, represented a fundamental shift from individual national actions to a coordinated global response by everyone with a responsibility to protect children from sexual abuse online. The Summit was led by the then Prime Minister and resulted in governments, technology companies and civil society organisations making concrete commitments to remove illegal images of children from the internet, identify and protect victims, and bring abusers to justice. A further Summit in 2015 was held in Abu Dhabi and focused on comprehensive national action and produced

a Model National Response, a tool to enable countries to assess the effectiveness of their response to online CSE. WePROTECT and the EU-US Global Alliance merged in 2015 to become the WePROTECT Global Alliance.

As part of the WePROTECT commitments made by industry, companies agreed to taking digital hashes or 'fingerprints' of known child sexual abuse material in order to identify this material on their platforms and services. By November 2016, approximately 36,000 Category A²⁴ hashes of known child sexual abuse material have been shared with six major companies by the Internet Watch Foundation.

Internet users in the UK, including members of the public, who find illegal images of child sexual abuse, and criminally obscene adult content, are able to report them to the Internet Watch Foundation (IWF). The web pages containing such images can be blocked by Internet Service Providers (ISPs).

The IWF is an independent organisation that acts as the UK hotline for the reporting of criminal content online. The purpose of the IWF is to minimise the availability of the following:

- child sexual abuse images hosted anywhere in the world;
- criminally obscene adult content hosted in the UK; and
- non-photographic child sexual abuse images hosted in the UK.

The IWF has authority to hold and analyse this content through agreement with the Crown Prosecution Service and the Association of Chief Police Officers. Since the IWF commenced proactive searching for child sexual abuse material in 2014 there has been a huge increase in the number of reports processed. In 2015, the IWF recorded 68,092 webpages containing child sexual abuse material which represents a 417% increase when compared to 2013 – the last full year before proactive searching started. If the site hosting the image is hosted in the UK, the IWF will pass the details to law enforcement (the Child Exploitation & Online Protection Centre Command of the National Crime Agency or local police forces) and the ISP will be asked to take down the webpage.

If outside the UK, the IWF will alert the hotline in the relevant country to enable them to work with law enforcement in that country to take down the webpage. In countries where a hotline does not exist, this liaison is carried out via INTERPOL. Although the IWF is not part of Government, the Home Office maintains regular contact with it, and retains the Ministerial lead on the issue of online child sexual exploitation. The responsibility for the legislation in respect of illegal indecent imagery of children and sexual contact with a child online sits with the Ministry of Justice.

During 2015, the IWF processed 112,975 reports – a 52% increase on 2014. Of the 112,975 reports processed in 2015, 68,543 were confirmed as containing criminal content by the IWF. This represents a 118% increase on 2014.

²⁴ Category A images depict the most serious category of offences as defined in the Sentencing Council's definitive guideline which can be accessed at: <https://www.sentencingcouncil.org.uk/news/item/update-to-sexual-offences-definitive-guideline/>

6 – Investigatory Powers

The use of a range of covert investigatory techniques is critical to law enforcement and the security and intelligence agencies' ability to counter the threats we face from terrorism, serious and organised crime, and state-based threats. This chapter explains key investigatory powers and describes the safeguards that apply to their use.

6.1 – Investigatory Powers Act 2016

The current legislative framework which governs investigatory powers, including the interception of communications and the acquisition of communications data, primarily consists of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Data Retention and Investigatory Powers Act 2014 (DRIPA). These ensure that these powers can only be used where it is necessary and proportionate to do so and for a specific set of purposes. In addition, DRIPA made clear the obligation set out in RIPA to comply with interception warrants applies equally to companies based in the United Kingdom and those overseas.

DRIPA was passed as emergency legislation in 2014 and was subject to a sunset clause which meant it expired at the end of December 2016. DRIPA also mandated that the Independent Reviewer of Terrorism Legislation, David Anderson QC, should review the legislative framework which provides for investigatory powers, and publish his report in a timeframe which could inform the development of new investigatory powers legislation before the expiry of DRIPA. As a consequence, the draft Investigatory Powers Bill was published in November 2015 for pre-legislative scrutiny.

The draft Bill was considered by the House of Commons Science and Technology Committee, the Intelligence and Security Committee of Parliament, and by a Joint Committee of both Houses of Parliament convened specifically to scrutinise this draft legislation. A revised Bill, which gave effect to the vast majority of the recommendations made by the three Committees, was introduced to Parliament in March 2016.

Following its consideration by both Houses of Parliament, the Investigatory Powers Act 2016 received Royal Assent on 29 November 2016.

The Act transforms the law relating to the use and oversight of investigatory powers, strengthening safeguards and introducing world-leading oversight arrangements. It does three things:

- First, it brings together powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It ensures that these powers – and the safeguards that apply to them – are clear and understandable.
- Second, the Act radically overhauls the way these powers are authorised and overseen. It introduces a ‘double-lock’ for the most intrusive powers, so that warrants cannot be issued by the Secretary of State until they have been approved by a Judicial Commissioner who must hold or have held high judicial office (e.g. have been a high court judge). And it creates a powerful new Investigatory Powers Commissioner (IPC) to oversee how these powers are used.
- Third, it ensures powers are fit for the digital age. The Act makes provision for the retention of internet connection records (ICRs) in order for law enforcement to identify the communications service to which a device has connected. This restores capabilities that have been lost as a result of changes in the way people communicate.

As the Investigatory Powers Act completed its passage through Parliament towards the end of 2016 and has not yet come into force, this report focuses on the exercise of investigatory powers under existing legislation.

Many of the Act’s provisions depend on the appointment of an Investigatory Powers Commissioner and Judicial Commissioners to approve warrants and notices, and to oversee the use of the powers. The Act also requires significant business change in the security and intelligence and law enforcement agencies. To manage this complex process, a phased programme to commence the powers in the Act has already begun, and more detail on progress in implementing the provisions in the Act will be made available in 2017.

6.2 – Overview of Interception

Interception is the power to obtain a communication in the course of its transmission. Interception by public authorities is currently provided for under the Regulation of Investigatory Powers Act 2000 and the Wireless Telegraphy Act 2006. The Investigatory Powers Act 2016, once implemented, will provide for the power to intercept and the relevant parts of RIPA and the Wireless Telegraphy Act 2006 will be repealed.

The use of interception, subject to strict controls and oversight, is a vital tool in the fight against terrorism, serious crime and other national security threats such as espionage. Terrorists increasingly use a range of communications services to radicalise, recruit and plan their attacks. Criminals use these services to commit crime and evade detection. The interception of the content of communications provides crucial intelligence on the plans and actions of terrorists and serious criminals, which allows law enforcement and the intelligence

agencies to disrupt or frustrate them. As highlighted by David Anderson QC, the Independent Reviewer of Terrorism Legislation, “*interception can be of vital importance for intelligence, for disruption, and for the detection and investigation of crime*”.²⁵ The majority of MI5’s priority investigations rely on interception in some form to identify, understand or disrupt plots seeking to harm the UK and its citizens.

The ability to obtain an interception warrant is only available to nine agencies. These are: the Security Service (MI5), the Secret Intelligence Service (SIS), the Government Communications Headquarters (GCHQ), the National Crime Agency (NCA), the Metropolitan Police Service (MPS), the Police Service of Northern Ireland (PSNI), the Police Service of Scotland, HM Revenue and Customs (HMRC), and the Ministry of Defence (MoD).

The National Technical Assistance Centre (NTAC) provides technical assistance to law enforcement and the security and intelligence agencies in relation to interception. NTAC does not itself apply for interception warrants. Rather, it manages the delivery of intercepted communications to the agencies that have a lawful authorisation in place to acquire them.²⁶

RIPA, and the Interception of Communications Code of Practice, sets out a comprehensive legal framework, approved by Parliament, for the regulation of the interception of communications. RIPA provides that an interception warrant must be authorised by a Secretary of State or Scottish Minister (dependant on the organisation applying for the warrant this will usually be: the Foreign Secretary, the Home Secretary, the Defence Secretary, the Secretary of State for Northern Ireland, or the Cabinet Secretary for Justice for Scotland). An interception warrant can only be authorised for limited and specified purposes, and only when the Secretary of State considers that it is both necessary and proportionate. Under the Investigatory Powers Act 2016, in addition to the Secretary of State (or Scottish Ministers), interception warrants will also need to be approved by a Judicial Commissioner before they can be issued.

Interception warrants authorise the interception of communication for three or six months. Where a warrant is authorised in the interests of national security or to protect the economic well-being of the UK (where it is directly linked to national security), it lasts for six months. Where a warrant is issued to prevent or detect serious crime, it lasts three months. An interception warrant may be renewed. An application to renew a warrant is considered in the same way as an application for new warrant. It must be authorised by a Secretary of State, and must still be considered to be necessary and proportionate. An interception warrant must be cancelled at any point if it is no longer necessary or proportionate.

At present, the use of interception is subject to independent oversight by the Interception of Communications Commissioner and the Interception of Communications Commissioner’s Office (IOCCO). The Commissioner reports to the Prime Minister and his reports are published and laid before Parliament (see also Chapter 8.2). Under measures in the Data Retention and

25 “A Question of Trust”, June 2015, can be accessed at: <https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/>

26 Further information on NTAC’s role is available at: <https://www.gchq.gov.uk/features/national-technical-assistance-centre>

Investigatory Powers Act 2014, the Commissioner is required to report on a twice yearly basis. His first half-yearly report was published on 8 September 2016 and his latest annual report, covering 2015, was published on 7 July 2016.

There are two types of interception warrant provided for in RIPA; one authorises targeted interception, the other bulk interception.

Targeted interception, currently authorised under section 8(1) of RIPA, is primarily an investigative capability and relates to obtaining the content of communications of a particular individual, group of individuals or single set of premises. **Bulk interception**, currently authorised under section 8(4) of RIPA, is a strategic intelligence gathering capability and usually involves the process of collecting a large volume of communications followed by the selection for examination of specific communications where it is necessary and proportionate for a particular statutory purpose. 8(4) warrants allow for the collection of communications of persons who are outside the UK in order to discover threats that could not otherwise be identified.

6.3 – 8(1) Warrants

Warrants issued under section 8(1) of RIPA may be issued to intercept communications to, or from, a specified person or premises carried on any postal service or telecommunications system. A section 8(1) warrant must name or describe either a person as the interception subject, or a single set of premises to which the interception warrant relates.

An application for a section 8(1) warrant will contain a consideration of necessity and proportionality, including:

- the background of the operation in question;
- the person or premises to which the application relates (and how the person or premises features in the operation);
- a description of the communications to be intercepted, details of the relevant communications service provider(s) and an assessment of the feasibility of the interception operation where this is relevant;
- a description of the conduct to be authorised or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data. This conduct may include the interception of other communications not specifically identified by the warrant as foreseen under 5(6)(a) of RIPA;
- an explanation of why the interception is necessary;
- consideration of why the conduct is proportionate to what is sought to be achieved by that conduct;
- consideration of any collateral intrusion and why that intrusion is justified in the circumstances;

- whether the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, or communications between a Member of Parliament and another person on constituency business;
- where an application is urgent, the supporting justification; and
- an assurance that all material intercepted will be handled in accordance with the safeguards required by section 15 of RIPA.

6.4 – 8(4) Warrants

Interception warrants may also be issued under section 8(4) of RIPA in respect of external communications. External communications are defined in RIPA as those which are sent or received outside the British Islands. They include those that are both sent and received outside the British Islands, whether or not they pass through the British Islands in the course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands in the course of their transmission, such as a domestic email that is transmitted via a server in another country.

Conduct authorised under a section 8(4) warrant may sometimes result in the incidental interception of communications that were both sent and received in the British Islands; RIPA permits this only if it is necessary to intercept the external communications that are the target of the warrant. In his 2015 Annual Report, the Interception of Communications Commissioner provided details of the interception warrants issued under 8(1) and 8(4) and the selection of material acquired under an 8(4) warrant.²⁷

As with an application for a section 8(1) warrant, an application for a section 8(4) warrant must contain a consideration of necessity and proportionality. Specifically, this will include:

- the background to the relevant operational requirement;
- a description of the conduct to be authorised, which must be restricted to the interception of external communications, or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data;
- a description of the communications to be intercepted, including details of the communications service provider(s) and an assessment of the feasibility of the operation where relevant;
- a consideration of why the conduct to be authorised by the warrant is necessary and proportionate to what is sought to be achieved by that conduct;
- an assurance that the intercepted material will be handled in accordance with the safeguards in RIPA; and
- an assurance that intercepted material will be read, looked at or listened to only so far as it is covered by the terms of a certificate issued by the Secretary of State

²⁷ This report is available at: www.iocco-uk.info

describing the material which may be examined. For example, a certificate might provide for the examination of material providing intelligence on terrorism (as defined in the Terrorism Act 2000) or on controlled drugs (as defined by the Misuse of Drugs Act 1971).

Responsibility for authorising any interception warrant, either under section 8(1) or section 8(4), lies with a Secretary of State or Scottish Ministers in the case of a Police Scotland warrant.

Before material intercepted under a section 8(4) warrant may be examined, it is subject to a further consideration of necessity and proportionality. If an analyst wishes to examine a communication sent by or intended for an individual believed to be located in the British Islands, he or she must apply to the Secretary of State for an authorisation under section 16(3) of RIPA. This process is similar to the application for a warrant under section 8(1).

Interception authorised under sections 8(1) and 8(4) plays a vital role in safeguarding national security and detecting and preventing serious crime.

An updated Interception of Communications Code of Practice was approved by Parliament in January 2016.²⁸ It includes new details about the operation of the regime for the interception of communications sent or received from outside the UK. It also includes further information about the safeguards for the interception of legally privileged communications and minor changes to reflect developments in the law since the Code was first introduced in 2002. A new Interception of Communications Code of Practice reflecting the powers in the Investigatory Powers Act 2016 will be published for public consultation in 2017.

Interception Statistics

There are statutory limits on the extent to which information can be published in relation to interception. Section 19 of RIPA requires that the existence of an interception warrant and steps taken to implement it, as well as any intercepted material, are kept secret. This reflects the importance of protecting the sensitive operational capabilities of law enforcement and the intelligence and security agencies. Publishing such details would assist those who seek to do us harm, including terrorists, to evade detection.

However, the Interception of Communications Commissioner does publish figures in relation to interception, including the total number of interception warrants authorised (see also Chapter 8.2). For 2015, this figure was 3,059. In 2014 it was 2,795, and in 2013, 2,760. The Commissioner's report also publishes the breakdown of the total number of warrants issued by statutory purpose. In 2015, 65% of warrants were issued for the purpose of the prevention and detection of serious crime compared to 68% in 2014, 34% were issued in the interest of national security compared to 31% in 2014, and 1% were issued in relation to a combination of statutory purposes in both years.

Warrants which were approved under the urgency procedure made up 2.5% of the total authorised for 2015. This means 80 warrants were approved in exceptionally urgent cases where, for example, there was an imminent, credible threat to national security, or a unique

²⁸ Available at: <https://www.gov.uk/government/publications/interception-of-communications-code-of-practice-2016>

opportunity to obtain intelligence to vital importance in relation to preventing or detecting a serious crime.

The annual report of the Interception of Communications Commissioner for 2015 highlighted that the total number of extant interception warrants as at 31 December 2015 was 1,518, a 5% decrease on 2014. Given that 3,059 warrants were authorised over the course of the year, this indicates that many interception warrants may be in place for no more than a matter of months. Of the 1,518 warrants that were extant at 31 December 2015, 22 were issued under section 8(4) of RIPA.

For the first time, the Commissioner's 2015 annual report made available the number of warrants which were subject to challenge or further information requests by senior officials or the relevant Secretary of State prior to their being approved, or that were rejected by the Secretary of State. On 64 occasions further information was requested, and on six occasions a Secretary of State refused an application for an interception warrant. The Commissioner's report makes clear that these figures relate to a mixture of new warrant applications, modifications and renewals, and hence should not be taken as a percentage of the 3,059 warrants issued in 2015.

6.5 – Targeted Communications Data

Communications data is information about who was communicating, when, from where, how and with whom; but not the content of a communication, what was said or written. For example, it can include the address to which a letter is sent; for mobile phones it might include location information, the time and duration of a phone call, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made; and for online communications, the internet protocol (IP) addresses identifying the individual who sent an email or posted a message on the internet, or the device that was used to make the communication.

Communications data is an essential tool for the full range of law enforcement activity and national security investigations. It enables the police, and other public authorities, to build a picture of the contacts and whereabouts of suspects and victims. Requests may be made for communications data in order to identify the location of a missing person or to establish a link (through call records) between a suspect and a victim. It is used to investigate crime, keep children safe, support or disprove alibis and tie a suspect to a particular crime scene, among many other things. Sometimes communications data is the only way to identify offenders, particularly where offences are committed online, such as child sexual exploitation or fraud. Communications data has played a role in every major Security Service counter-terrorism operation over the past decade. It can also be used in evidence and has been used in 95% of all serious organised crime prosecution cases handled by the Crown Prosecution Service.

The acquisition of communications data is stringently regulated, primarily by RIPA. RIPA ensures that communications data can only be acquired by certain public authorities for a statutory purpose. For example, the police can acquire communications data in an emergency to help locate someone whose life is at risk but where no crime is suspected. Applications

for communications data must be authorised by a designated person in a relevant public authority, and can only be authorised where necessary and proportionate in relation to a specific investigation from which the designated person is independent. In the case of local authorities, since 1 December 2014, applications must be made centrally through the National Anti-Fraud Network (NAFN) and, under provisions in the Protection of Freedoms Act 2012, also require judicial approval. The power to acquire communications data under RIPA was removed from 13 authorities in 2015.

The Data Retention and Investigatory Powers Act 2014 (DRIPA) ensured the availability of certain categories of communications data to public authorities when needed. DRIPA, and the Data Retention Regulations 2014 made under it, introduced additional safeguards, enhancing our data retention notice regime and formalising the requirements placed on communications service providers to safeguard this data. The Counter-Terrorism and Security Act 2015 (CTSA) amended DRIPA, enabling the retention of additional information to assist in identifying the person who was using an IP address at a specific point in time.

The relevant provisions in DRIPA and CTSA have been repealed and replaced by provisions in Part 4 of the Investigatory Powers Act 2016. This addresses the growing capability gap caused by the pace of technological change which has limited the ability of law enforcement to identify the sender of online communications or the internet services being used by a suspect or a missing person. The relevant provisions in RIPA will be replaced by provisions in Part 3 of the Investigatory Powers Act once the statutory oversight body is fully established. The Investigatory Powers Act will ensure that there is a legal framework that is modern, fit for purpose and gives our law enforcement and intelligence agencies the capabilities they need.

The Interception of Communications Commissioner ('the Commissioner') and the Interception of Communications Commissioner's Office (IOCCO) provide independent oversight of the acquisition of communications data by public authorities, including through inspections of these authorities. The Commissioner provides reports to the Prime Minister, which are subsequently published. The latest annual report of the Commissioner was laid before Parliament on 8 September 2016.

The processing of personal information, including communications data, is regulated by the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and is overseen by the Information Commissioner. The Information Commissioner is also under a duty to audit compliance by communications service providers with the provisions of the Data Retention Regulations 2014 with respect to the security, integrity and deletion of retained data.

Two codes of practice, both revised in March 2015, provide guidance on the procedures to be followed when acquiring, disclosing or retaining communications data under the legislation described here. The Acquisition and Disclosure of Communications Data Code of Practice sets out rules for the granting authorisations to acquire data, the giving of notices to require disclosure of data and the keeping or records, including records of errors.

Following the Commissioner's report into the use of communications data to identify journalistic sources published in February 2015, this Code was revised in March 2015

to introduce a requirement that law enforcement acquisition of communications data to determine journalistic sources be carried out under the Police and Criminal Evidence Act 1984 (or equivalent legislation in Northern Ireland and Scotland), which provides for judicial authorisation.

The Retention of Communications Data Code of Practice sets out how the Government implements the requirements in DRIPA and the Data Retention Regulations and covers: the issue, review, variation and revocation of data retention notices; the communications service providers' ability to recover their costs; data security; oversight by the Information Commissioner; and safeguards on the disclosure and use of retained data by communications service providers. A new Code of Practice will be published for public consultation in 2017. It will reflect changes to the interception powers and safeguards as provided for by the Investigatory Powers Act 2016.

Communications Data Statistics

The Commissioner's latest annual report covering 2015 contains extensive detail on the use of communications data by public authorities, as outlined below (see also **Chapter 8.2**).

Following concerns that the statistical requirements levied on public authorities did not allow for reliable comparisons of the actual amount of communications data acquired, new provisions were introduced in March 2015 through the Acquisition and Disclosure of Communications Data Code of Practice requiring public authorities to record and provide the Commissioner with statistics relating to the number of items of data acquired, as well as the number of applications made, authorisations granted and notices given.

In his Report for 2015, the Commissioner published the number of items of data acquired, rather than data previously published in relation to applications, authorisations and notices. These new figures improve transparency by providing a realistic assessment of the use of the powers and enable more accurate comparisons to be drawn between public authorities. Whilst they provide a more accurate representation of the amount of communications data acquired, these figures will also be a considerably larger number than the number of applications, authorisations or notices and are not directly comparable with figures published in previous years.

Due to the timing of the introduction of this requirement, the data included in the Commissioner's annual report includes some projected or partial figures, based on the available information. However, the Commissioner is confident that the projections provide a more accurate picture of use than the previous limited statistical requirements. The figures provided here are subject to the statistical limitations detailed in the Commissioner's Report.

761,702 items of communications data were acquired by public authorities under Chapter II of Part I of RIPA in 2015. An item of data is a request for data on a single identifier or other descriptor: for example, 30 days of incoming and outgoing call data in relation to a mobile telephone would be counted as one item of data. As this statistic was not collated in previous years, it is not possible to draw statistical comparisons with previous reports.

This statistic replaces those that previously counted the number of authorisations granted and notices given to acquire communications data under section 22 of RIPA. It also replaces those statistics which previously counted the total number of applications made for communications data.

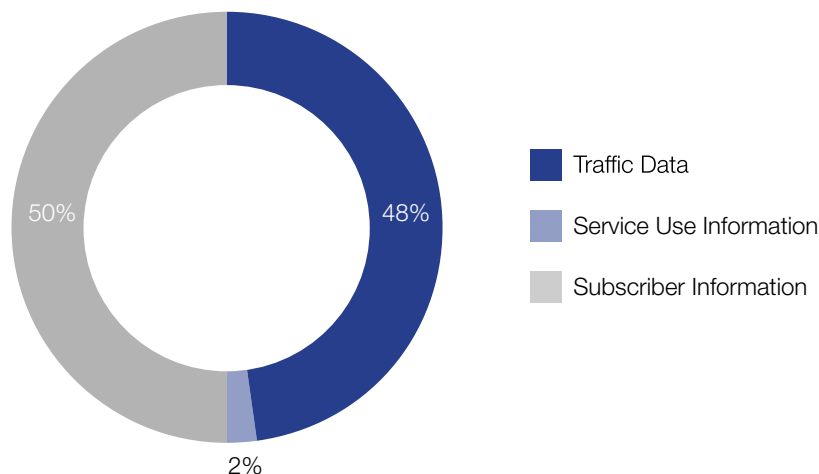
In certain circumstances, and where there is no time to complete the normal written process for requesting communications data, a public authority may make an urgent oral request. Circumstances where an urgent oral request may be made include a situation where there is an imminent threat to life, or where there is a credible threat to national security. During 2015, 11% of applications to acquire communications data were approved orally. After the period of urgency, a written process must be completed, demonstrating the consideration given to the circumstances and the decisions taken. In addition, written notice must be given to the relevant communications service provider retrospectively, but within one working day, of the oral notice being given. Failure to do so constitutes an error, which must be recorded by the public authority that made the request.

The Commissioner's 2015 report includes details of the total number of items of communications data acquired, broken down in a number of ways. First, it includes a breakdown by data types acquired, in relation to the three data types at section 21(4) of RIPA. Traffic data, at section 21(4)(a), is data about a communication and the equipment used in transmitting it, such as information about the location of a mobile phone, or the IP address used to communicate over the internet. Service use data, at section 21(4)(b), is information about the use a person makes of a communications service and might include itemised telephone call records, or whether someone has diverted their telephone. Subscriber data, at section 21(4)(c), is information held by a communications service provider about people to whom they provide a service (such as their name, address and telephone number).

There are statutory restrictions on the categories of communications data that public authorities can access. For example local authorities cannot access traffic data.

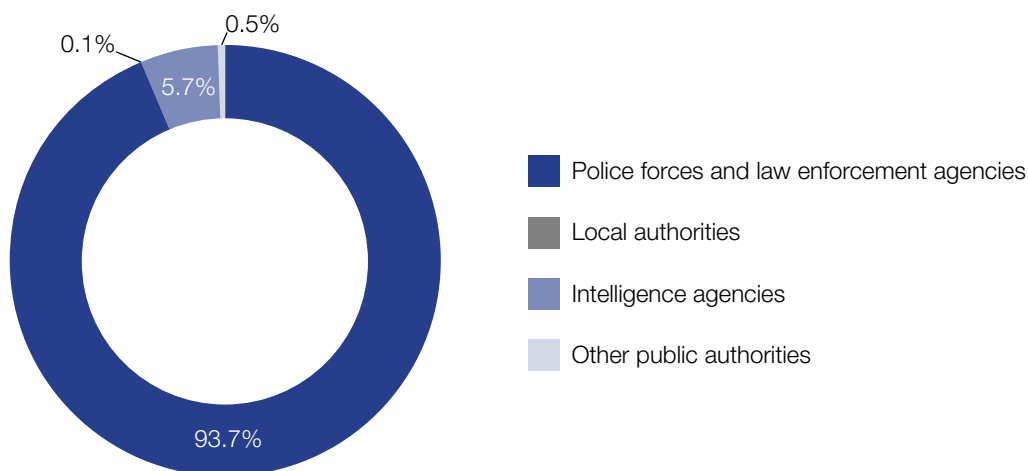
In 2015, 50% of communications data acquired was subscriber data; 48% was traffic data; and 2% was service use data. The majority of items of data acquired (82.6%) related to telephony identifiers, such as landline or mobile phone numbers; 14.1% related to internet identifiers, such as email addresses or IP addresses; 0.8% related to postal identifiers, such as postal addresses; and the remaining 2.5% related to "other" identifiers, such as bank account or credit card numbers.

Figure 3: Communications data acquired by data type, 2015



The Commissioner's report also breaks down the total number of items of data acquired, except those granted on an urgent oral basis, by the type of public authority requesting the data. This shows that the large majority of communications data requests made in 2015 were from the police and law enforcement agencies, comprising 93.7% of total communications data acquired. The security and intelligence agencies accounted for 5.7% of the total, and less than 1% was acquired by local authorities (0.1%) and other public authorities (0.5%).

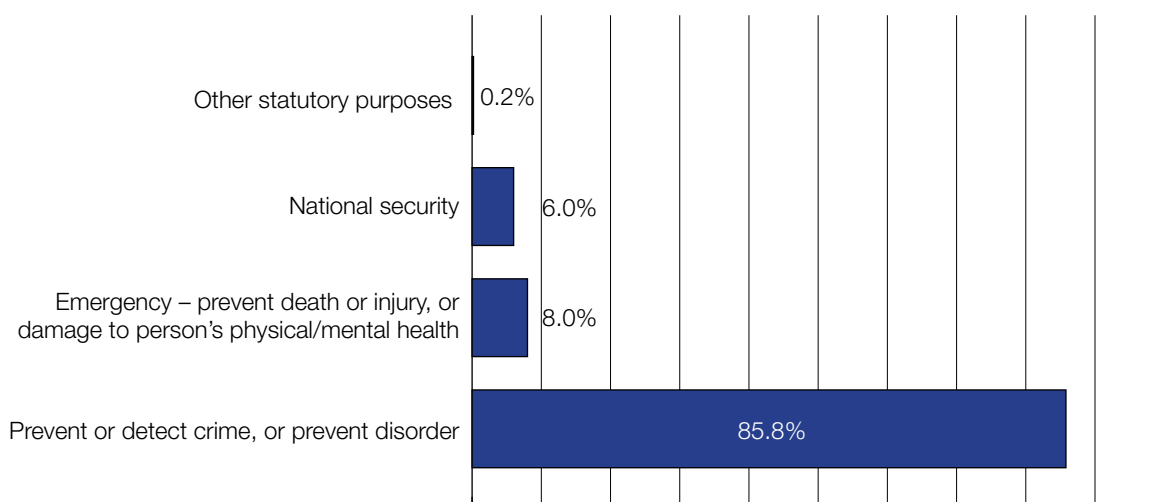
Figure 4: Communications data acquired by public authority type, 2015



The report also breaks this category down further, and includes the total number items of data approved by each public authority. The full list is included at **ANNEX C**.

The Commissioner's report also breaks down the total number of items of data by the statutory purpose for which it was acquired. During 2015, the prevention and detection of crime or prevention of disorder (section 22(2)(b) of RIPA) was the statutory purpose for which communications data was most often acquired, accounting for 85.8% of communications data acquired. The next most common statutory purposes were preventing death or injury in an emergency situation (8%) (section 22(2)(g) of RIPA) and national security (6%); the combined total for all other statutory purposes accounted for 0.2% of communications data acquired.

Figure 5: Communications data applications by statutory purpose, 2015



The Commissioner's report previously did not include statistics on the number of individuals to whom communications data notices and authorisations related. The reasons for this were explained in last year's report. The new statistical requirement levied on public authorities now requires public authorities to record, for each item of data, whether that item relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation.

As a result we are able to report that during 2015, 70% of applications to acquire communications data related to criminal suspects or persons of interest for national security purposes. Approximately 10% of the requests related to victims, complainants or witnesses. It is believed that the proportion of data relating to vulnerable persons is under-represented in these figures due to the use of urgent oral requests to trace vulnerable missing persons. IOCCO consider that it is likely that the vulnerable person category would be of parity with the victim and associate categories.

6.6 – Bulk Communications Data Acquisition

The security and intelligence agencies use a range of techniques under existing legislation to acquire information in volume. This information, sometimes referred to as ‘bulk data’, is used to generate intelligence about threats that cannot be acquired by more targeted means.

Section 94 of the Telecommunications Act 1984 (‘Section 94’) provides a power for the Secretary of State to issue directions ‘of a general character’ to communications service providers in the interests of national security or relations with the government of a country or territory outside the United Kingdom. Directions given under this power enable the agencies to obtain communications data in bulk from telecommunications operators, where the Secretary of State considers that such a direction is proportionate to what is sought to be achieved.

The use of this power to provide for bulk communications data acquisition was avowed in November last year, when in the interests of transparency the then Home Secretary, the Rt. Hon. Theresa May MP, set out its existence in a statement in the House of Commons, saying:

“The [draft Investigatory Powers] Act will make explicit provision for all of the powers available to the security and intelligence agencies to acquire data in bulk. That will include not only bulk interception provided under the Regulation of Investigatory Powers Act 2000 and which is vital to the work of GCHQ, but the acquisition of bulk communications data, both relating to the UK and overseas. That is not a new power. It will replace the power under Section 94 of the Telecommunications Act 1984, under which successive Governments have approved the security and intelligence agencies’ access to such communications data from communication service providers.”

At the same time, in the absence of a provision to publish a Code of Practice relating to the exercise or performance and duties under Section 94 directions, the security and intelligence agencies published their joint Arrangements for the Acquisition of Bulk Communications Data Pursuant to Directions under Section 94 of the Telecommunications Act 1984.

Copies of directions given in relation to bulk communications data acquisition have not been laid before Parliament as the Secretary of State considers it is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person to do so.

The Government recognises the need to deliver greater openness and transparency in the Investigatory Powers arena. The Investigatory Powers Act will replace Section 94 with a clear, transparent power subject to enhanced safeguards. The enhanced safeguards for these powers include a ‘double lock’, where a Judicial Commissioner has to approve the Secretary of State’s decision to issue a warrant, and the creation of a powerful new Investigatory Powers Commissioner to oversee their use.

Fast, secure access to communications data is essential to the agencies in pursuing their investigations. The ability to acquire and access this data in bulk, subject to strict safeguards

and oversight, is vital to the agencies' effectiveness, providing unique intelligence that the agencies cannot obtain by any other means. In some cases bulk communications data may be the only investigative lead that the agencies have to work with.

It is clear that these capabilities have helped to protect the UK. The analysis of bulk data, for example, has:

- played an important part in every major counter terrorism investigation of the last decade, including in each of the 12 plots disrupted in the past three years;
- enabled over 90% of the UK's targeted military operations during the campaign in the south of Afghanistan;
- been essential to identifying 95% of the cyber-attacks on people and businesses in the UK discovered by the agencies over the last six months; and
- been used to identify serious criminals seeking to evade detection online, and who cannot be pursued by conventional means, supporting the disruption of over 50 paedophiles in the UK in the last three years.

Bulk communications data is therefore among the most important tools that the security and intelligence agencies can use to obtain intelligence on subjects of interest, including threats to UK citizens and our Armed Forces; identify threats here in the UK, sometimes from fragments of intelligence; establish and investigate links between known subjects of interest, at pace, in complex investigations; understand known suspects' behaviour and communications methods to identify potential attack planning; verify information obtained about subjects of interest through other sources (e.g. agents); and resolve sometimes anonymous online personae to real-world identities.

While the security and intelligence agencies can also make individual communications data requests to communication service providers under RIPA, the ability to access data in bulk is critical, because it enables the agencies to conduct searches, where necessary and proportionate, across all the relevant data, in a secure way. This enables more complex analysis to be undertaken, particularly when the results are matched against other data holdings. By using bulk communications data, links can be established that would be impossible or significantly slower (potentially taking many days) to discover through a series of individual requests to communication service providers. This can sometimes be the difference between identifying and disrupting a plot, and an attack taking place.

Bulk communications data acquisition capabilities were first used at scale in the UK in 2001 after the 9/11 attacks in New York, and later extended following the attacks on the London transport system on 7 July 2005 to respond to the domestic terrorist threat. They are regularly used alongside other capabilities to investigate known, high-priority threats and to identify emerging threats from individuals not previously known to the security and intelligence agencies. This crucial investigative tool allows the agencies to:

- identify and investigate potential threats in complex and fast-moving investigations;

- conduct more sophisticated analysis, by ‘joining the dots’ between individuals involved in planning attacks, often working from fragments of intelligence obtained about potential attacks;
- narrow down likely targets much more quickly, so that they can focus limited investigative resource where it is really needed, quickly ruling out other associates and family members from an investigation, and minimising intrusion into the privacy of those who are not of intelligence interest; and
- reduce the risk of an incomplete intelligence picture which makes it difficult to assess the entirety of a threat posed by a known subject – a point made forcefully in the report by the Intelligence and Security Committee of Parliament into the murder of Fusilier Lee Rigby in 2013.

Within the UK, the analysis of bulk communications data is often the only way for the agencies to progress investigations and identify terrorists from very limited lead intelligence, or when their communications have been deliberately concealed.

The responsibility for issuing directions under Section 94 rests with the Secretary of State. Directions are only issued where it is both necessary and proportionate to do so. Each direction must be clearly justified and balance intrusions into privacy against the expected intelligence benefits. Robust internal safeguards apply in relation to the accessing of material acquired under such directions. The handling arrangements for data acquired under Section 94 were published alongside the draft Investigatory Powers Bill in November 2015, and a draft Bulk Acquisition Code of Practice was published in March 2016, when the Bill was introduced into Parliament.

The security and intelligence agencies conduct internal six-monthly reviews of directions issued under Section 94 to acquire communications data in bulk in order to assess whether the reasons and justifications for the directions remain valid. Conclusions are submitted to the Secretary of State. The operators are also informed of their obligations to continue to comply with Section 94 directions.

When a Section 94 direction to disclose bulk communications data is no longer required, the security and intelligence agencies inform both the Secretary of State and the relevant telecommunications operator. Where there is a requirement to modify or cease a Section 94 direction, a submission is sent to the Secretary of State setting out the justification for the change and the agency consults with the telecommunications operator in the same way as it would with a new Section 94 direction.

Oversight of these powers is conducted by the Interception of Communications Commissioner. In January 2015 the then Prime Minister asked the then Interception of Communications Commissioner to formally oversee all directions given by a Secretary of State under Section 94, excluding those given to telecommunications operators relating to the work of the Office of Communications (Ofcom) or on behalf of the Department of Business, Innovation and Skills (BIS). This includes directions given under Section 94 in relation to bulk communications data acquisition, as well as directions given for other purposes. Further details may be found in Section 7.2.

Bulk Communications Data Acquisition Statistics

Section 94 does not provide for any requirement for record keeping in relation to directions given under this power or the use of any communications data acquired in bulk under such directions. Since commencing oversight of directions given under this power in early 2015, the Commissioner has instigated record-keeping requirements. The Investigatory Powers Act 2016 will introduce record-keeping requirements in line with those currently in place for the targeted acquisition of communications data under RIPA.

The Commissioner's Report of his review of directions given under Section 94 includes those statistics currently available on the acquisition of communications data in bulk by the agencies, as outlined below (see also **Section 7.2**).

At the time the review took place, there were fifteen extant section 94 directions relating to the acquisition of bulk communications data. A number of the directions have been modified over the years, for example, to expand or to cease the acquisition of certain data, and this has led in some instances to the direction being re-issued.

Only GCHQ and the Security Service use Section 94 directions to acquire bulk communications data. In 2015, GCHQ identified 141,251 communications addresses or identifiers of interest from communications data acquired in bulk pursuant to Section 94 directions which directly contributed to an intelligence report.

In 2015, the Security Service made 20,042 applications to access communications data obtained pursuant to Section 94 directions. These applications related to 122,579 items of communications data. The Commissioner concluded that overall the Security Service applications examined were submitted to an excellent standard and satisfied the principles of necessity and proportionality.

All of the extant requirements for bulk communications data are for traffic data as defined in section 21(4)(a) of RIPA. All of the current directions require regular feeds of bulk communications data to be disclosed by the relevant telecommunications operator.

One operator had historically been required (since 2001) to supply subscriber information to GCHQ in addition to traffic data as part of a section 94 direction. This requirement ceased in August 2015 after an internal review and the subscriber information obtained was destroyed. The agency handling arrangements for the acquisition of bulk communications data published in November 2015 state clearly that: *"The communications data collected is limited to "Traffic Data" and "Service Use Information...The data provided does not contain communication content or Subscriber Information..."*

All of the Section 94 directions specified that they were necessary under section 94(1) of the Telecommunications Act 1984 *"in the interests of national security"*. None of the Section 94 directions specified that they were necessary for *"relations with the government of a country or territory outside the United Kingdom"*.

6.7 – Covert Surveillance, Covert Human Intelligence Sources and Property Interference

The use of a range of covert techniques is an important weapon in the fight against terrorism and serious and organised crime, including the trafficking of drugs and firearms, and child abuse. Covert surveillance (both intrusive and directed surveillance) and the use of covert human intelligence sources (CHIS) are regulated by Part II of the Regulation of Investigatory Powers Act 2000 (RIPA). Additionally, the Police Act 1997,²⁹ and the Intelligence Services Act 1994,³⁰ provide for property interference to be undertaken by the law enforcement and intelligence agencies, where necessary and proportionate, in accordance with the strict criteria set out in those Acts.

The use of all of these powers is subject to rigorous independent oversight. The exercise of these powers by the security and intelligence agencies and the Ministry of Defence is overseen by the Intelligence Services Commissioner (see also **Section 7.3**). The use of these powers by the police and other public authorities is overseen by the Office of Surveillance Commissioners (see also **Section 7.4**).

Intrusive Surveillance

Intrusive surveillance is surveillance which takes place inside residential premises or private vehicles, whether by human or technical means. The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained.

Only a limited number of public authorities are able to undertake this type of surveillance and its use is robustly safeguarded. Intrusive surveillance can only be conducted in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interest of the economic well-being of the UK.

When consideration is being given to the authorisation of intrusive surveillance, there must be a consideration as to whether the information sought could reasonably be acquired by other means. Any application by the security and intelligence agencies, the Ministry of Defence and HM Armed Forces requires authorisation by the Secretary of State. Applications by the police and other public authorities are authorised internally at Chief Constable or equivalent level. However, these applications additionally require the prior approval of an independent Surveillance Commissioner.

Directed Surveillance

Directed surveillance is covert surveillance conducted at any location (including online), other than within residential premises or private vehicles, that is likely to result in the obtaining of private information about a person. A wider group of public authorities, including local authorities, can undertake this form of surveillance. Authorisation is obtained from a senior

29 The Police Act 1997 is available at www.legislation.gov.uk/ukpga/1997/50/contents

30 The Intelligence Services Act 1994 is available at www.legislation.gov.uk/ukpga/1994/13/contents

designated person within the organisation and can only be granted where necessary and proportionate, for a specific statutory purpose, and in relation to an individual investigation.

Local authorities in England, Wales and Northern Ireland³¹ must also obtain judicial approval for the use of directed surveillance, under measures in the Protection of Freedoms Act 2012.³² In addition to seeking judicial authorisation, local authorities in England and Wales may only make use of directed surveillance in relation to the investigation of criminal offences which attract at least a six month sentence, or in relation to offences relating to the sale of alcohol or tobacco to children.

Covert Human Intelligence Sources

A covert human intelligence source (CHIS) is anyone who is asked by a public authority to start or maintain a relationship for a covert purpose. This includes undercover officers employed by the public authority, or members of the public acting as informants. Provisions in RIPA ensure that the use of a CHIS may only be authorised at a suitably senior level where necessary and proportionate for a statutory purpose approved by Parliament. Local authorities must also obtain judicial approval for use of CHIS. In addition, section 29 (4) of RIPA sets out further safeguards regarding the use of a CHIS, including the requirement that a qualifying person in the relevant public authority must have day-to-day responsibility for dealing with the CHIS, and for the CHIS's security and welfare.

The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 increased the authorisation levels required before an undercover officer can be deployed and enhanced oversight by the Office of Surveillance Commissioners. Specifically, any deployment of an undercover law enforcement officer must be authorised by an Assistant Chief Constable, or equivalent, and notified to the Office of Surveillance Commissioners. Any deployment which lasts more than 12 months must be authorised directly by the Chief Constable, or equivalent, and must be approved by a Surveillance Commissioner. This same level of authorisation and approval must be obtained for any authorisation lasting more than three months where the authorisation involves matters subject to legal privilege.

Property Interference

Property interference may be authorised for law enforcement agencies with an authorisation issued under Part III of the Police Act 1997. This allows them to enter or interfere with property, or wireless telegraphy, for the purpose of preventing or detecting serious crime. Similar powers are available to the security and intelligence agencies under section 5 of the Intelligence Services Act 1994.

Property interference is subject to a stringent authorisation regime, ensuring it can only be used where it is necessary and proportionate and where the desired outcome cannot be achieved by other means. In the case of law enforcement agencies, an authorisation can only

31 In Northern Ireland this requirement only applies to authorisations where the grant or renewal relates to a Northern Ireland excepted or reserved matter. Where such an authorisation is required by a local authority in Northern Ireland, an application for a grant or renewal should be made to a district judge.

32 The Protection of Freedoms Act is available at www.legislation.gov.uk/ukpga/2012/9/contents

be obtained from a Chief Constable, or equivalent. Where a member of a law enforcement agency authorises property interference, he or she must, as soon as reasonably practical, inform a Surveillance Commissioner. In addition, prior approval for a property interference authorisation must be sought from a Surveillance Commissioner where the property in question is used wholly or mainly as a dwelling or is a hotel bedroom or office premises. Approval by a Surveillance Commissioner is also required where the interference might involve acquiring knowledge of matters subject to legal privilege, journalistic material or confidential personal information.

The security and intelligence agencies require a warrant signed by the Secretary of State to conduct property interference. The Secretary of State may only authorise a warrant where he or she is satisfied that it is necessary and proportionate, and he or she must also consider whether the relevant information could be reasonably obtained by other means. In many cases, an operation using covert techniques may involve both directed or intrusive surveillance and property interference, such as where a covert device needs to be placed inside a residential property for the purpose of conducting intrusive surveillance. This can be authorised as a combined authorisation, although the specific criteria for authorisation of each activity must be considered separately.

Under the Investigatory Powers Act 2016, interference with equipment such as computers and mobile devices currently authorised under property interference powers, will be authorised by an equipment interference warrant where it is carried out for the purpose of acquiring communications, information or equipment data with a British Islands connection, and if a Computer Misuse Act offence would otherwise be committed. Further information about these powers is provided at Section 6.8 below. Interference with equipment that is not for the purpose of obtaining communications, information or equipment data, e.g. where the purpose of the interference is to disable the equipment, will continue to fall under existing property interference powers. Interference with other forms of property and with wireless telegraphy will not be affected by this change and will continue to be authorised under the existing property interference powers.

Codes of Practice

The Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice provide guidance to public authorities on the use of these powers. The Codes are issued under section 71 of RIPA and public authorities are required under the Act to have regard to the Codes. Both Codes were updated in 2014 to reflect, among other things, the enhanced authorisation procedures for law enforcement agencies' use of CHIS, and for local authorities' use of directed surveillance and CHIS. Also, the revised CHIS Code stipulates that all police officers in England and Wales must comply with and uphold the principles and standards of professional behaviour set out in the College of Policing Code of Ethics, introduced in July 2014.

The Code of Ethics states clearly that covert tactics must be appropriately authorised and any deployments must be shown to be proportionate, lawful, accountable, necessary and ethical. The Code of Ethics also states that officers must not establish or pursue an improper sexual

or emotional relationship with a person with whom they come into contact in the course of their work who may be vulnerable to an abuse of trust or power.

Both the above Codes of Practice will be revised following enactment of the Investigatory Powers Act 2016 to reflect the relevant changes in that legislation.

Statistics for covert techniques

Security and Intelligence Agencies

The annual report of the Intelligence Services Commissioner includes statistics on the total number of warrants and authorisations approved for the security and intelligence agencies and Ministry of Defence (see also **Section 7.3**).

At the end of 2015, the total number of extant warrants and authorisations was 1,560.

Law Enforcement Agencies and Other Public Authorities

The annual report of the Chief Surveillance Commissioner includes statistics on the use of intrusive surveillance, directed surveillance, CHIS and property interference by law enforcement agencies and other public authorities (see also **Section 7.4**). The Commissioner's latest report covers the period 1 April 2015 to 31 March 2016. It advises that there were 289 authorisations for intrusive surveillance, compared to 321 in the previous period. None were quashed by Commissioners during the year.

Law enforcement agencies authorised the use of directed surveillance on 7,118 occasions, with 1,057 extant at the end of March 2016. These figures were lower than in the previous reporting period, where the Commissioner reported that 8,333 authorisations were given, with 1,173 extant at the end of the year. The total number of authorisations for directed surveillance by other public authorities was 2,029, a small reduction from 2,207 the previous year. These figures fit into a continuing downward trend of the use of directed surveillance by these authorities. The Department for Work and Pensions (DWP) continues to account for the majority of authorisations within this category. The number of directed surveillance authorisations given by the DWP during this reporting period increased from 894 to 1,258.

During the reporting period, 2,239 CHIS were authorised by law enforcement agencies and as at 31 March 2016, there remained 2,275 authorised, including some which may have been authorised in preceding years. Over the course of the year, 2,206 CHIS authorisations were cancelled. In addition to this, 1,155 "relevant sources" (better known as undercover officers) were notified to the Office of Surveillance Commissioners, 902 were cancelled and 72 were submitted for the prior approval renewal process.³³ At the end of the reporting period, there were 62 active CHIS in other public authorities. Only a very small proportion of these public authorities (3%) use CHIS. This will often be for matters such as trading standards investigations.

³³ These figures represent the number of times a single individual undercover officer has been authorised for deployment on a specific police operation. As such, the total number of authorisations does not reflect the number of undercover operations undertaken during the year.

During the reporting period, and excluding renewals, property interference authorisations were granted on 2,070 occasions. This was a decrease of 21 on the previous year. None of these authorisations were quashed by Commissioners.

Figure 6: Summary of key activity in relation to the use of covert techniques in the year ending 31 March 2016

| | Intrusive surveillance authorisation | Property interference authorisation | Relevant sources notified | Directed surveillance authorisation | Authorised CHIS at 31/03/2015 |
|---------------------------------|---------------------------------------------|--------------------------------------------|----------------------------------|--------------------------------------------|--------------------------------------|
| Law Enforcement | 289 | 2,070 | 1,155 | 7,118 | 2,275 |
| Other Public Authorities | | | | 2,029 | 62 |

6.8 – Equipment Interference

Equipment interference allows the security and intelligence agencies, law enforcement agencies and the armed forces to interfere with electronic equipment such as computers and smartphones in order to obtain data, such as communications from a device. Equipment interference encompasses a wide range of activity from remote access to computers, to downloading covertly the contents of a mobile phone during a search.

Where necessary and proportionate, law enforcement agencies and the security and intelligence agencies need to be able to access communications or other information held on devices, in order to gain valuable intelligence in national security and serious crime investigations and to help gather evidence for use in criminal prosecutions. The armed forces use equipment interference with the support of the security and intelligence agencies in some situations to gather data in support of military operations. Equipment interference plays an important role in mitigating the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption and other attempts to evade detection. It can sometimes be the only method by which to acquire the data.

Equipment interference is currently used by law enforcement agencies and the security and intelligence agencies; more sensitive and complex techniques are generally available only to the security and intelligence agencies and a small number of law enforcement agencies, including the National Crime Agency. Equipment interference is currently provided for under general property interference powers in the Intelligence Services Act 1994 and the Police Act 1997. A Code of Practice was published earlier this year which governs the current use of equipment interference by the security and intelligence agencies.

Building on recommendations made by David Anderson QC and the Intelligence and Security Committee of Parliament, the Investigatory Powers Act 2016 provides for a new, more transparent equipment interference regime that will govern the use of these techniques by law enforcement agencies, the security and intelligence agencies and the armed forces, introducing new, enhanced safeguards. The use of this power is limited to the same statutory

purposes as interception. Law enforcement agencies' use of equipment interference will be permitted for the prevention and detection of serious crime and preventing death or preventing or mitigating any injury or damage to a person's physical or mental health.

Use of these powers by the security and intelligence agencies currently requires authorisation by the Secretary of State. This will continue under the Investigatory Powers Act 2016. Under the Act, authorisations for law enforcement agencies may be issued by the relevant law enforcement chief, typically a Chief Constable. The Act will also strengthen authorisation safeguards so that the issue of warrants will, in future, also be subject to approval by a Judicial Commissioner.

The use of equipment interference powers is currently overseen by the Intelligence Services Commissioner and Surveillance Commissioners. The Commissioners ensure that the safeguards set out in the legislation and accompanying codes of practice are stringently applied and that appropriate arrangements are in place to handle the material obtained. The Commissioners audit how the authorities use the power and report publicly on what they find. As set out in his annual report for 2015, the Intelligence Services Commissioner requires that the agencies designate a senior official responsible for engaging with the Commissioner during inspections and overseeing implementation of any post inspection action plans. As required by the Equipment Interference Code of Practice 2016, the Intelligence Services Commissioner gives particular consideration to cases where the subject of an operation might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information includes confidential personal information, confidential journalistic material, communications subject to legal privilege or communications between a Member of Parliament and another person on constituency business.³⁴

The Investigatory Powers Commissioner will oversee the use of equipment interference powers by law enforcement, the security and intelligence agencies, and the armed forces once the Investigatory Powers Act 2016 is implemented.

6.9 – Investigation of Protected Electronic Information

The ability to investigate electronic information protected by encryption is an important tool for the security and intelligence and law enforcement agencies. Information security technologies, from the use of passwords to advanced cryptography, enable businesses and individuals to protect their electronic data when going about their lawful business. However, terrorists and criminals use the same technologies in order to conceal their conduct and to evade detection.

Part III of RIPA enables a notice to be served on a holder of protected electronic information requiring them to put that information into an intelligible form, where the information has been lawfully obtained by a public authority. This may include, for example, requiring a suspect in a criminal investigation to provide the password to their mobile phone where it has been seized by the police.

³⁴ The Commissioners' reports can be found in full at intelligencecommissioner.com and osc.independent.gov.uk

The use of these powers is subject to stringent safeguards. Permission to require that protected information is put into an intelligible form may only be granted where necessary and proportionate. These powers can only be exercised in the interests of national security, to prevent or detect crime, or in the interests of the economic well-being of the UK. In addition, these powers must not be used where the person with the appropriate permission can obtain possession of the protected information in an intelligible form without the giving of a notice.

Schedule 2 of RIPA sets out additional safeguards relating to the giving of a notice. A person may only serve a notice in relation to protected information if they have been granted permission by a relevant authority in accordance with Schedule 2.

The National Technical Assistance Centre (NTAC), which provides technical assistance to public authorities, particularly law enforcement agencies and the security and intelligence agencies, includes a facility for the processing of lawfully obtained protected electronic information.

NTAC is the lead national authority for matters relating to the processing of protected information into an intelligible form, and acts as a guardian and gatekeeper to public authorities that have powers to exercise this function.

A public authority may seek permission for giving a notice from an appropriate authority. The authority from whom permission will be sought depends on the legal mechanism by which the protected information came into the possession of the public authority.

Where protected information has been, or is likely to be, obtained under a warrant issued by a person holding judicial office, public authorities may obtain appropriate permission from such a person holding judicial office. Such permission might be granted, for example, in relation to a production order obtained under the Police and Criminal Evidence Act 1984.

Where protected information is likely to be, or has been, obtained under a warrant issued by the Secretary of State, for example an interception warrant, appropriate permission for giving a notice in respect of that information may be obtained from the Secretary of State.

Where protected information is likely to be, or has been, obtained through an authorisation under Part III of the Police Act 1997 (authorisation of otherwise unlawful action in respect of property) appropriate permission for giving a notice may be obtained from an authorising officer within the meaning of that Act.

The Police, National Crime Agency, HMRC and members of HM forces have appropriate permission, without a requirement for to seek permission from a judicial authority or Secretary of State, in relation to protected information in certain circumstances. This is the case where that information is likely to be, or has been, obtained by the exercise of a statutory power and is not information obtained under a warrant issued by the Secretary of State or a person holding judicial office, or an authorisation under Part III of the Police Act 1997, or information obtained by the intelligence agencies. For example, this could be in relation to information obtained under section 19 of the Police and Criminal Evidence Act 1984, which relates to a constable's general powers of seizure.

Once appropriate permission has been granted, a notice can be given, imposing a disclosure requirement. The effect of imposing a disclosure requirement is that the recipient shall be required, in accordance with the notice, to provide for the protected information in his or her possession to be put into an intelligible form. RIPA makes it an offence if the recipient knowingly fails, in accordance with the notice, to make the required disclosure, and if the recipient fails to keep the existence of such a notice secret.

Statistics on the investigation of protected electronic information

The annual report of the Chief Surveillance Commissioner includes details of the number of investigations into protected electronic information. The Commissioner's latest report covers the period from 1 April 2015 to 31 March 2016. The report outlines that during the reporting period, NTAC granted 87 approvals, out of 88 applications, to investigate electronic data protected by encryption. The Annual Report of the Interception of Communications Commissioner confirms that there were no notices given in 2015 for the investigation of protected electronic information, in relation to information obtained from an interception warrant.

6.10 – Bulk Personal Datasets

Bulk Personal Datasets (BPDs) are sets of personal information about a large number of individuals, the majority of whom will not be of any interest to the security and intelligence agencies. The datasets are held on electronic systems for the purposes of analysis in the security and intelligence agencies. Examples of these datasets include the telephone directory or the electoral roll.

BPDs are essential in helping the security and intelligence agencies identify subjects of interest or individuals who surface during the course of an investigation, to establish links between individuals and groups, to understand better a subject of interest's behaviour and connections and quickly to exclude the innocent. In short, they enable the agencies to join the dots in an investigation and to focus their attention on individuals or organisations that threaten our national security.

BPD Case Study: Preventing Access to Firearms

The terrorist attacks in Mumbai in 2008 and the more recent shootings in Copenhagen and Paris in 2015, highlight the risk posed from terrorists gaining access to firearms. To help manage the risk of UK based subjects of interest accessing firearms, the intelligence agencies match data about individuals assessed to have access to firearms with records of known terrorists. To achieve this, the security and intelligence agencies acquired the details of all these individuals, even though the majority will not be involved in terrorism and therefore will not be of direct intelligence interest. This allowed the matching to be undertaken at scale and pace, and more comprehensively than individual requests could ever achieve. Completing such activities enabled the security and intelligence agencies to manage the associated risks to the public.

Regulation and Oversight

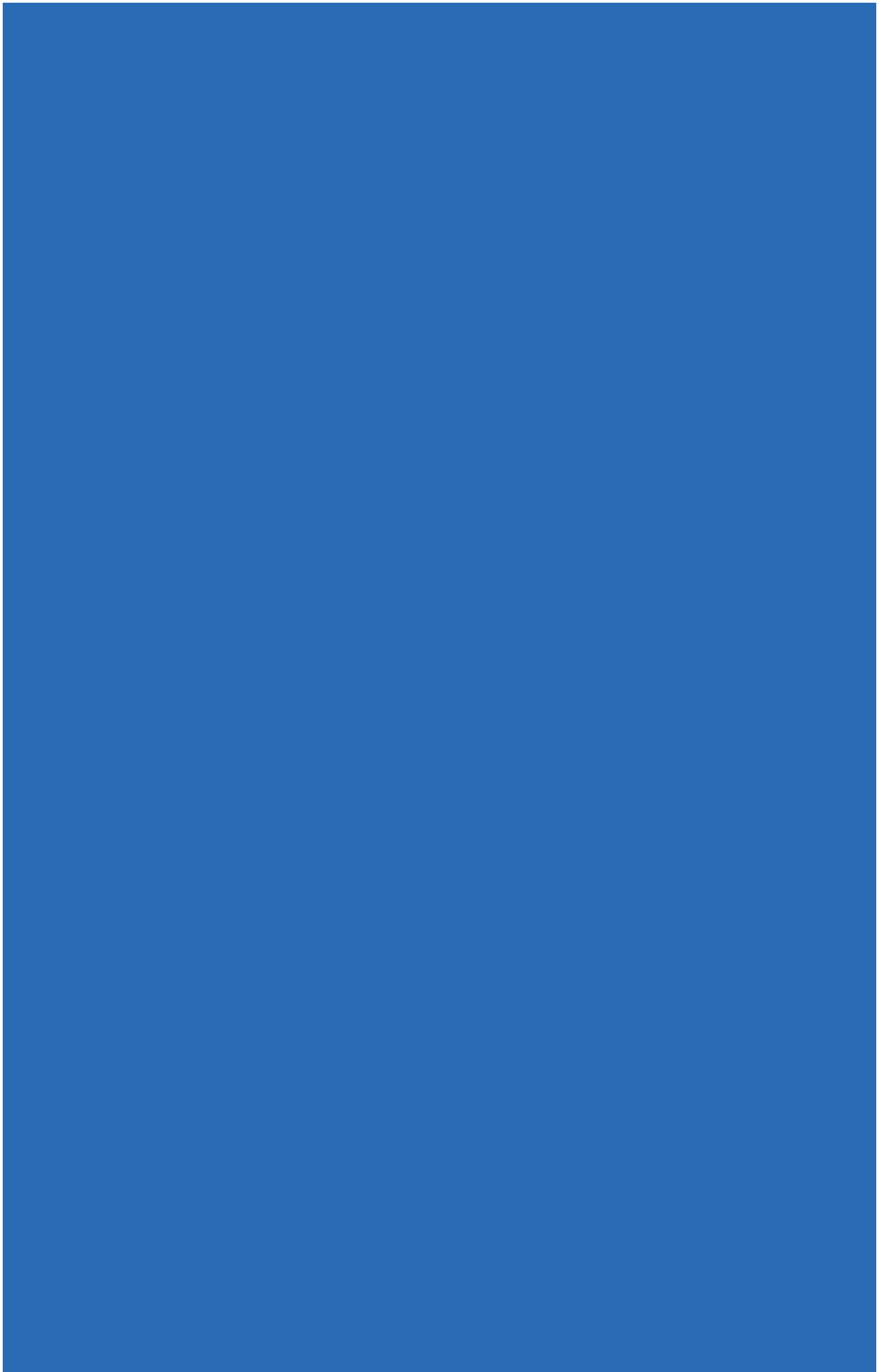
The security and intelligence agencies have powers under the Security Service Act 1989 and the Intelligence Services Act 1994 to acquire and use BPDs to help them fulfil their statutory functions, including protecting national security. BPDs may be acquired using investigatory powers, from other public sector bodies or commercially from the private sector. The use of BPD is subject to stringent internal handling arrangements and the regime is overseen by the Intelligence Services Commissioner.

In his 2015 Report, the Intelligence Services Commissioner, the Rt Hon Sir Mark Waller, outlined the process by which BPDs are inspected. The Commissioner is given access to a list of the BPDs held by each agency including: a short description of each dataset; the date it was acquired; the date it was ingested onto an analytical system; an assessment of the levels of intrusion and corporate risk associated with the BPD; when the BPD was last reviewed by a review panel; and if and when the Commissioner last inspected the BPD. From this list, the Commissioner selects a number of datasets at random to inspect in further detail. At the inspection, all relevant documents and records in relation these datasets are scrutinised. The Commissioner also speaks to the individuals responsible for the dataset and reviews all of the policies relevant to BPD, including minutes from recent review panels.

The Commissioner's 2015 Report also highlighted that in addition to oversight by the Commissioner, the security and intelligence agencies have a number of internal oversight mechanisms which include controls such as completing mandatory training, adhering to codes of practice, and signing terms and conditions before access is granted. The agencies also conduct internal monitoring and audits. This includes the audit of the individual search justifications at SIS and GCHQ.

The Investigatory Powers Act 2016 will enhance the safeguards that apply to the retention and examination of BPDs acquired under the Security Service Act 1989 and the Intelligence Services Act 1994. The Secretary of State will have to approve warrants for the retention and examination of BPDs if it is necessary and proportionate to do so. As will be the case for interception and equipment interference authorisations, a Judicial Commissioner must also approve the warrant.

A statutory Code of Practice will provide guidance on the procedures that must be followed before BPDs can be retained and examined by the security and intelligence agencies. The Investigatory Powers Commissioner will oversee how the agencies use these datasets. Supported by a team of Judicial Commissioners and technical and legal experts, the Commissioner will audit how the agencies use them and they will report publicly on what they find.



7 – Oversight

As well as being stringently regulated by the robust safeguards set out in existing legislation, the use of disruptive and investigatory powers is subject to rigorous, independent oversight. The UK's system of oversight for law enforcement and the security and intelligence agencies' use of investigatory powers is provided for in different Acts of Parliament. These include the Regulation of Investigatory Powers Act 2000 (RIPA), the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A), the Police Act 1997, and the Justice and Security Act 2013 (JSA).

Oversight of the powers and their use is carried out by a number of different bodies. Independent, non-Parliamentary oversight is carried out by:

- the Interception of Communications Commissioner (IoCC) who oversees how public authorities use interception and communications data powers under RIPA and powers under section 94 of the Telecommunications Act;
- the Chief Surveillance Commissioner (CSC) who oversees how law enforcement agencies use covert surveillance powers and covert human intelligence sources under RIPA Part II and the Police Act 1997; and
- the Intelligence Services Commissioner (ISCom) who oversees how the intelligence agencies use the powers available to them under RIPA Part II (covert surveillance and covert human intelligence sources) and the Intelligence Services Act 1994.

In addition, the operation of terrorism legislation, including the exercise of various disruptive powers set out in this report, is subject to review by the Independent Reviewer of Terrorism Legislation.

Lastly, the Investigatory Powers Tribunal (IPT) provides an independent right of redress to any individual who believes that investigatory powers have been used unlawfully against them.

The following section explains the roles and functions of each of the Commissioners, as well as the Independent Reviewer of Terrorism Legislation and the Investigatory Powers Tribunal, setting out their inspection and reporting regimes, and outlining the findings of their most recent annual reports.

Further to the oversight bodies that are explained below, parliamentary oversight of the work of the security and intelligence agencies is conducted by the Intelligence and Security Committee of Parliament (ISC). The ISC was established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of the Security Service, Secret

Intelligence Service and GCHQ. The Justice and Security Act 2013 provided the Committee with additional powers, increasing its remit to include retrospective oversight of operational activity (when it is in the national interest) and the wider intelligence and security activities of Government.

The Investigatory Powers Act 2016

The system of non-parliamentary oversight will change during the next year following the passage of the Investigatory Powers Act 2016 through Parliament.³⁵ Once implemented, the Act will create a single new independent and more powerful Investigatory Powers Commissioner. The Commissioner will have a significantly expanded role in authorising the use of investigatory powers and a wide-ranging and self-determined remit to oversee how law enforcement and the security and intelligence agencies use the powers and capabilities available to them.

The Commissioner will be a senior judge and with their supporting staff will have three key roles. Firstly, they will authorise and approve the use of investigatory powers. Judicial Commissioners, who will hold or have held high judicial office (i.e. a judicial office at least as senior as a High Court judge) will undertake this role. Secondly, they will have an inspection role. The Commissioner will audit compliance and undertake investigations. Judicial Commissioners will undertake this role and will be supported by a team of expert inspectors.

Thirdly, the new Commissioner will have a clear mandate to inform Parliament and the public about the use of investigatory powers. The Commissioner will report publicly and make recommendations on what they find in the course of their work. The Commissioner will also publish guidance when it is required on the proper use of investigatory powers. The Commissioner will have a strong public profile and active media and online presence so that they are quickly established as an authoritative source of advice and information. To support these three roles, the Commissioner will also have dedicated legal, technical and communications support.

The Act will also strengthen the right of redress by allowing a domestic right of appeal from the Investigatory Powers Tribunal to the Court of Appeal or the Court of Session on points of law.

An Investigatory Powers Commissioner has yet to be appointed. Further detail on the role and appointment of the Investigatory Powers Commissioner will be set out in the next iteration of the Transparency Report.

7.1 – Independent Reviewer of Terrorism Legislation

The role of the Independent Reviewer of Terrorism Legislation (“the Independent Reviewer”), David Anderson QC, is to ensure that the operation of UK counter-terrorism legislation is fair, effective and proportionate. As part of this role, the Independent Reviewer regularly writes reports which are presented to Secretaries of State and subsequently laid before

³⁵ http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf

Parliament and published, thereby informing public and political debate. He is independent of Government and is security cleared to access the most sensitive information relating to national security.

The Independent Reviewer's statutory functions are set out at section 36 of the Terrorism Act 2006. They require him to review the operation of a broad range of terrorism legislation, including some of the powers covered elsewhere in this report.³⁶

This remit includes, at its heart, reviewing on an annual basis the operation of the core Terrorism Acts – the Terrorism Act 2000 which sets out much of our legislative framework on terrorism, and Part 1 of the 2006 Act which contains some of the core terrorism offences. The Independent Reviewer's reports on these two Acts cover the following areas:

- definition of terrorism;
- proscribed organisations;
- terrorist property;
- terrorist investigations;
- arrest and detention;
- stop and search;
- port and border controls; and
- terrorism offences.

Changes made in the Counter-Terrorism and Security Act 2015 increased the number of statutes which the Independent Reviewer is responsible for overseeing, but also increased the flexibility and autonomy with which he may do so. From 2016, the Independent Reviewer is required to provide the Home Secretary with a work programme at the beginning of each calendar year, specifying what he will report on in that 12 month period. He has discretion to set his work programme based on where he considers he should focus his attention, with the exception of the core Terrorism Acts on which the annual reporting requirement outlined above remains. The Secretary of State may also ask the Independent Reviewer to undertake other ad hoc or snapshot reviews (see below).

In addition to these standing responsibilities which form the core of his role, the Independent Reviewer has also carried out other one-off statutory reviews. Section 66 of the Immigration Act 2014 provides a power to deprive a person of their British nationality where this may leave them stateless, and also requires the Secretary of State to appoint a person to carry out a review of the operation of this power within a year of its enactment (and then at subsequent three-year intervals). The Independent Reviewer was asked to undertake this initial review, and his report was published on 21 April 2016.

36 All of the Independent Reviewer's reports can be found on his website:
www.terrorismlegislationreviewer.independent.gov.uk

The Data Retention and Investigatory Powers Act 2014 required the Secretary of State to appoint the Independent Reviewer to conduct a one-off review of the operation and regulation of investigatory powers, and report his findings to the Prime Minister. This report, titled 'A Question of Trust', was published on 11 June 2015, and greatly informed the debate around the Investigatory Powers Act 2016. The review gave specific consideration to the following issues:

- current and future threats to the UK;
- the capabilities needed to combat those threats;
- safeguards to protect privacy;
- the challenges of changing technology;
- issues relating to transparency and oversight; and
- the effectiveness of existing legislation (including its proportionality) and the case for new or amending legislation.

Following this, in June 2016 the Government asked the Independent Reviewer to carry out a further review of the bulk powers in the Investigatory Powers Act 2016 (then the Investigatory Powers Bill) and provide a report to the Prime Minister. The review examined the operational case for bulk interception, bulk equipment interference, bulk acquisition of communications data, and bulk personal datasets. The Independent Reviewer, and a team of his choosing, critically appraised the need for bulk capabilities, including consideration of whether the same result could have been achieved through less intrusive means. The Government provided complete access to the most sensitive information to enable the review to be undertaken effectively.

The Independent Reviewer's report was laid in Parliament and published on 19 August 2016. The report concluded that "*bulk powers play an important role in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield*". The review also concluded that where alternatives exist to the use of bulk powers: "*they are often less effective, more dangerous, more resource-intensive, more intrusive or slower*".

This review was published during the passage of the Investigatory Powers Act 2016 and was vital to informing its parliamentary scrutiny.

The Government publishes responses to the Independent Reviewer's reports and his recommendations. The most recent response to his Annual Report on the operation of the Terrorism Acts was published on the GOV.UK website on 8 November 2016.³⁷

7.2 – Interception of Communications Commissioner

The Interception of Communications Commissioner is appointed by the Prime Minister under section 57 of the Regulation of Investigatory Powers Act (RIPA). The Rt Hon Sir Anthony May

³⁷ <https://www.gov.uk/government/publications/government-response-to-the-annual-report-on-the-operation-of-the-terrorism-acts-in-2014>

stepped down as Commissioner on 31 July 2015 and The Rt Hon Sir Stanley Burnton was appointed on 4 November 2015. In the interim between appointments, the Interception of Communications Commissioner's Office (IOCCO) continued to undertake audits of public authorities' use of interception and communications data.

The Interception of Communications Commissioner is independent of Government and must hold, or have held, high judicial office in order to be appointed to the role. The Commissioner's primary role is to oversee the use of two investigatory tools, interception and communications data (see also Sections 5.1 to Chapter 5.6), and to ensure that the Secretaries of State and public authorities operating under Part I of RIPA, which regulates the use of these powers, do so lawfully. Specifically, the Commissioner's statutory responsibilities under section 57(2) of RIPA are to keep under review:

- the exercise and performance by the Secretary of State of the powers and duties in sections 1 to 11 of RIPA, that is those relating to the granting and operation of interception warrants;
- the exercise and performance by the Scottish Ministers of the powers and duties conferred and imposed by sections 5, 9 and 10 of RIPA;
- the exercise and performance by the persons on whom they are conferred or imposed of the powers and duties under Chapter II Part I (RIPA), that is those relating to the acquisition and disclosure of communications data;
- the exercise and performance by the Secretary of State in relation to information under Part 1 of the powers and duties conferred or imposed by or under Part 3 of RIPA, and
- the adequacy of arrangements for safeguards relating to use that is made of interception material under section 15 (RIPA), which also embraces additional safeguards in section 16 (RIPA) so far as applicable to Part I material, those imposed by section 55.

Section 58(1) of RIPA imposes a statutory obligation on everyone concerned with the lawful interception of communications and the acquisition and disclosure of communications data under RIPA Part I to disclose or provide to the Commissioner all such documents or information as they may require for the purpose of enabling the Commissioner to carry out their functions under section 57.

In addition to his statutory responsibilities under RIPA, the Commissioner also conducts oversight, by non-statutory agreement, of the lawful interception of prisoners' communications under section 47 of the Prison Act 1952 within prisons in England, Wales and Northern Ireland.

At the behest of the former Prime Minister, the Commissioner also has responsibility for conducting non-statutory oversight of Section 94 of the Telecommunications Act 1984. Specifically, this oversight will cover the necessity and proportionality of any directions given by the Secretary of State under Section 94, the use of any such directions and the safeguards that apply to them. Further information about directions given under this power,

including those which enable the agencies to obtain communications data in bulk from telecommunications operators, may be found in Chapter 6.

The Commissioner does not have oversight of matters that are overseen by the Intelligence Services Commissioner, Sir Mark Waller (see also Section 6.3), and the Chief Surveillance Commissioner, the Rt Hon the Lord Judge (see also Section 6.4).

Under section 58(4) of RIPA, the Commissioner is required, as soon as practicable after the end of each calendar year and at the end of the period of six months beginning with the end of each calendar year, to report to the Prime Minister on the exercise of his functions. These reports are subsequently published and laid before Parliament.

The most recent annual report of the Commissioner, covering January to December 2015, was published on 8 September 2016 and contained more detailed information and statistics than ever before in relation to the use of the investigatory powers that he oversees. The report was published in full with no confidential annex. The statistics regarding the use of interception and communications data, are set out in Chapter 6.1 to Chapter 6.6 of this report. In addition to his 2015 Annual Report, the Commissioner's second half-yearly report was published on 7 July 2016. The main purpose of this report was to review directions issued under section 94 of the Telecommunications Act 1984.³⁸

A significant proportion of IOCCO's effort in 2016 focused on providing details of experiences, observations, concerns and findings to the three independent reviews on the use of investigatory powers by law enforcement and the intelligence and security agencies. These reviews informed the public and political debate around the use of these powers and, critically, the drafting of the Investigatory Powers Act 2016.

IOCCO also publishes a number of guidance documents, circulars, press statements and inquiry reports on its website in order to provide the public with as much information as possible about its functions.³⁹ In addition, IOCCO has provided guidance to the IPT on a number of cases this year, and advice to public authorities in light of changes to existing Codes of Practice relating to powers overseen by the Commissioner.

Interception

The Commissioner's 2015 Annual Report sets out details of the rigorous processes that his office, IOCCO, undertake to ensure that interception powers are being used lawfully and in accordance with RIPA. This includes inspections of the intercepting agencies and warrant granting departments. During 2015, IOCCO carried out 26 inspections of public authorities. There are three primary objectives during these inspections, which are to ensure:

- that the systems in place for the interception of communications are sufficient for the purposes of Part I Chapter I and that all relevant records have been kept;
- that all interception has been carried out lawfully, and in accordance with Part I Chapter I of RIPA, and the associated Code of Practice; and

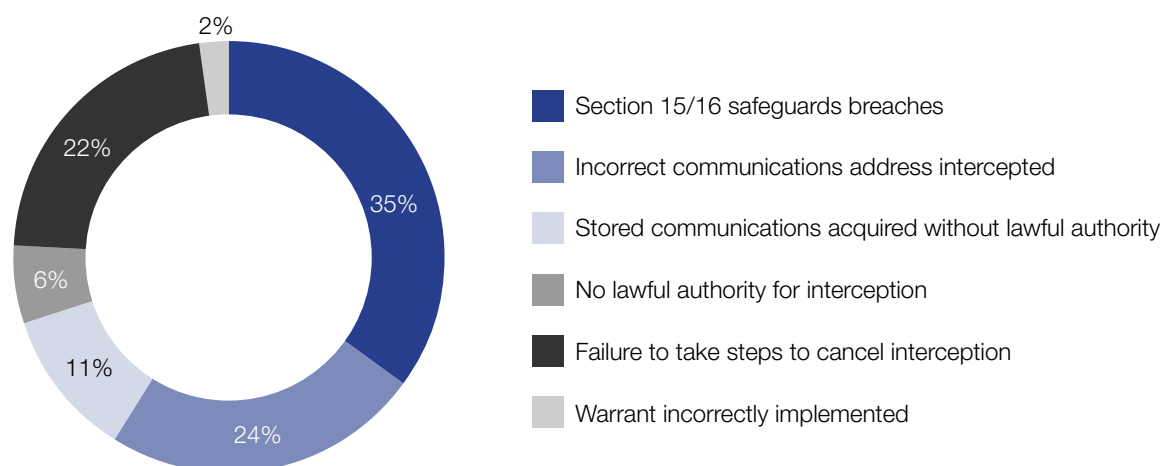
38 The Commissioner's reports can be found in full at www.iocco-uk.info

39 www.iocco-uk.info

- that any errors are reported to the Commissioner and that the systems are reviewed and adapted where any weaknesses or faults are identified.

Over the course of these inspections, IOCCO examined 1,148 interception warrants, including associated paperwork. Following each inspection, IOCCO provides an inspection report to the head of the agency or department, outlining the formal recommendations. The relevant agency is required to report back to IOCCO within two months of this report, outlining the progress against these recommendations. The total number of recommendations made to the agencies and departments in 2015 was 74. During 2015, 62 errors were reported to IOCCO in relation to interception. The breakdown of the causes of these errors is outlined below.

Figure 7: Summary of causes of errors reported to IOCCO in relation to interception in 2015



The largest category of errors was in relation to the “section 15/16 safeguards breaches”. These are instances where communications have been lawfully intercepted but where resultant actions do not comply with the safeguards in RIPA. An example of such an error would be an error in a technical system causing unwanted data to be selected for examination.

Communications Data

During 2015, IOCCO undertook 72 communications data inspections. Of these 72 inspections, 53 were of police forces and law enforcement agencies, three were of a security and intelligence agency, and 15 were of other public authorities and the National Anti-Fraud Network (NAFN) who act as the Single Point of Contact for all local authorities. Since 1 December 2014, all local authority requests for communications data must be made through NAFN. As a consequence the Commissioner no longer inspects individual local authorities but accesses those records at NAFN. During the NAFN inspection, 71 local authorities who had submitted applications in 2015 were inspected.

The primary objectives of the communications data inspections are to ensure:

- that the systems in place for acquiring communications data are sufficient for the purposes of RIPA and that all relevant records have been kept;
- that all acquisition of communications data has been carried out lawfully and in accordance with Part I Chapter II and its associated Code of Practice;
- that the data acquired was necessary and proportionate to the conduct authorised;
- that errors are being “reported” or “recorded” and that the systems are reviewed and adapted in light of any weaknesses or faults that are exposed; and
- that persons engaged in the acquisition of communications data are adequately trained and are aware of the relevant parts of the legislation.

Over the course of these 72 inspections, IOCCO scrutinised at random approximately 15,000 applications and over 117,000 applications were subject to query-based examinations. Where they are inspecting public authorities that only make a small number of applications, IOCCO will generally examine all applications that are made. For larger users, a random sample will be taken. In addition, a larger sample set is examined using query-based searching methods. As with interception inspections, IOCCO completes a report following each inspection, outlining recommendations, which the public authority is required to respond to within two months. From the 72 inspections in 2015, the total number of recommendations made was 366.

The Acquisition and Disclosure of Communications Data Code of Practice sets out two types of communications data error. A recordable error is one that does not result in communications data being wrongly acquired. Such errors must be recorded and made available to IOCCO during an inspection. A reportable error is one which results in data being wrongly acquired. Such errors must be reported to the Commissioner within five working days of the error being discovered.

In total, 1,199 communications data errors were reported to the Commissioner during 2015, this is an increase of 20% on the 998 errors reported in 2014. As the majority of errors are self-reported it is difficult to comment whether this represents greater vigilance in the spotting of errors; less care being taken; or relates to the type of data being acquired. A comparison with the 2014 figures reveals that the main cause for the overall rise is a larger number of incorrect communications identifiers being submitted by applicants and single points of contact⁴⁰ (“SPoCs”) within authorities, or data being acquired over the incorrect date or time period.

During 2015, 41% of errors identified were caused by the applicant and 43% by SPoCs by, for instance, including the incorrect communications address or date/time period on the application. 13% of errors were caused by communications service providers, for instance by disclosing the incorrect type of data or excess data, and 3% by designated persons.

40 The single point of contact (SPoC) is an accredited individual trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and communications service providers.

At the end of each inspection, the public authority is given an overall compliance rating of good, satisfactory or poor. In 2015, 78% of public authorities achieved a good compliance rating, compared to 80% in 2014. In addition, 18% received a satisfactory rating, an increase of 4% from 2014 and only 4% of public authorities received a poor rating in 2015, a decrease of 2% from 2014.

Of the 1,199 errors in 2015, 23 serious errors were identified. IOCCO defines the following as serious errors:

- technical errors relating to communications service providers secure disclosure systems which result in a significant number of erroneous disclosures;
- errors where the public authority has, as a consequence of the data, initiated a course of action that impacts on persons not connected with the investigation or operation (for example, the sharing of information with another public authority stating a person is suspected of a crime, an individual being visited or the execution of a search warrant at premises unconnected with the investigation, the arrest of a person); and
- errors which result in the wrongful disclosure of a large volume of communications data or a particularly sensitive data set.

Of the 23 serious errors, 14 were caused by human mistakes and nine were as a result of technical system faults.

IOCCO identified four investigations where data had been acquired to identify or determine journalistic sources without judicial authorisation. In relation to two of those investigations, the Commissioner decided the conduct was such that the affected parties should be informed. In one case the Commissioner determined that the conduct was reckless and the affected individuals subsequently made complaints to the Investigatory Powers Tribunal (IPT). In the second case the Commissioner determined that two applications were not necessary or proportionate.

Each of these errors is extremely regrettable. The Government welcomes the rigorous approach IOCCO have taken in their investigations to establish the causes of these errors, and to provide recommendations to mitigate the chances of recurrence.

The total of 1,199 errors in 2015, including the 23 serious errors, should be viewed in the context of the total number of items of communications data acquired: 761,702 for 2015.

Bulk Communications Data Acquisition

Since commencing oversight of Section 94 in January 2015, the Commissioner has conducted formal inspections on an annual basis at any public authority for which the Secretary of State has given section 94 directions for the acquisition of bulk communications data. At present this is only the Security Service and GCHQ.

These inspections include investigation into:

- the giving of Section 94 directions by the Secretary of State, including a review of the judgements made by the Secretary of State and the security and intelligence agency relating to necessity and proportionality;
- whether the policies and procedures in place at the security and intelligence agency for the acquisition, storage, access to, disclosure, retention and destruction of bulk communications data are sound and provide adequate safeguards against misuse;
- the process of serving of Section 94 directions on telecommunications operators, including the prior consultations and subsequent communication between the agencies and operators;
- the procedures in place between the operator and a security and intelligence agency for the secure acquisition, storage and disclosure of the bulk communications data, including verification that the data disclosed accords with the direction given;
- the retention and destruction arrangements in place at a security and intelligence agency; and
- the controls in place to prevent and detect misuse of bulk communications data.

In conducting his investigations, the Commissioner will also review any errors reported to him by the relevant security and intelligence agency, and the measures put in place by that agency to prevent any potential recurrence.

There is no statutory requirement to report an error when undertaking the acquisition of bulk communications data by means of a Section 94 direction or when accessing data already retained as a consequence. However, the Security Service has implemented an internal policy process to report instances they consider to be errors when accessing communications data retained as a consequence of a Section 94 direction.

Between 1 January 2015 and the date of the completion of the Commissioner's report on Section 94 directions, which was published on 7 July 2016,⁴¹ the Security Service reported 230 errors, the majority of which were the result of a failure to comply with the Security Service's handling arrangements and internal policies.

The Commissioner's investigation into this series of errors concluded that they represented contraventions of the handling arrangements. However, the Commissioner also reported that:

- communications data accessed in these instances was accessed for legitimate purposes;
- the case to access the communications data was made orally and was authorised by a designated person prior to the data being accessed; and
- there was no evidence that the applications which were completed retrospectively did not meet the tests of necessity or proportionality.

⁴¹ The Commissioner's report can be found in full at www.ioocco-uk.info

Whilst GCHQ have a mechanism for reporting errors to the Commissioner, they cannot easily differentiate the source from which the data is derived without compounding any potential intrusion (for example, by re-running the erroneous query) due to the fact that they commonly merge the communications data obtained under a Section 94 direction with other datasets containing communications data (for example, related communications data obtained as a consequence of an interception warrant).

GCHQ has not reported any errors to the Commissioner that relate specifically to data obtained under a Section 94 direction.

Any error made in the acquisition of communications data, whether in bulk or as targeted data, is extremely regrettable. The Government welcomes the rigorous approach the Commissioner has taken in inspecting the use of data acquired under Section 94 directions since he commenced oversight of this power in 2015.

7.3 – Intelligence Services Commissioner

The Intelligence Services Commissioner, the Rt Hon Sir John Goldring, was appointed by the Prime Minister under section 59 of the Regulation of Investigatory Powers Act 2000 (RIPA) on 1 January 2017. He replaced the Rt Hon Sir Mark Waller who stood down on 31 December 2016.

The Commissioner is independent of Government and is responsible for providing independent, external oversight of the use of intrusive powers by the UK security and intelligence agencies and parts of the Ministry of Defence (MoD). The Justice and Security Act 2013 conferred additional functions on the Intelligence Services Commissioner requiring him to keep under review the carrying out of any aspect of the functions of the security and intelligence agencies, as directed by the Prime Minister (except for anything that is required to be kept under review by the Interception of Communications Commissioner; for example the Intelligence Services Commissioner is not responsible for oversight of directions under section 94 of the Telecommunications Act 1984).

The statutory functions of the Commissioner are set out in section 59 of RIPA. The Commissioner's statutory functions can be broken down into the following main areas:

- to keep under review the exercise by the Secretary of State and Scottish Ministers of their powers to issue warrants and authorisations to enable the security and intelligence agencies to carry out their functions. Such warrants and authorisations can relate to entering onto or interfering with property (or with wireless telegraphy), equipment interference, intrusive surveillance, and the investigation of electronic data protected by encryption;
- to keep under review the exercise and performance of the powers and duties imposed on the intelligence services and MoD/armed forces personnel in relation to covert activities, which are the subject of an internal authorisation procedure. Such activities include directed surveillance, the conduct and use of covert human intelligence sources (CHIS), and the investigation of electronic data protected by encryption;

- to keep under review compliance with the Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees (direction dated 27 November 2014);
- to advise the Home Office on the propriety of extending the Terrorism Prevention and Investigation Measures (TPIMs) regime;
- to provide oversight of the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets (BPD) by the intelligence services including misuse of data and how this can be prevented (direction dated 11 March 2015); and
- to keep under review the carrying out of any other aspect of the functions of the security and intelligence agencies, HM Forces or the MoD as directed by the Prime Minister.

The Commissioner is also required to provide the Prime Minister with an annual report on the discharge of his functions, which the Prime Ministers lays before Parliament.⁴² The Commissioner's latest report covers 2015. As part of his continued drive for greater openness, the Commissioner restructured his report last year to address issues thematically including, for example, sections on intrusive surveillance, directed surveillance, covert human intelligence sources and Intelligence Services Act section 7 authorisations. This year the thematic sections were expanded to include additional information about bulk personal datasets and, for the first time, equipment interference. The Report provided greater statistical detail than previous iterations and also reported on how the agencies and the Commissioner work together to mitigate the risk of abuse of powers by any individual, or group of individuals.

In order to acquire the information required to meet his statutory functions, the Commissioner scrutinises how the security and intelligence agencies and MoD carry out their activities. This scrutiny includes oversight audits of each of the security and intelligence agencies that are able to apply for and authorise warrants (the Security Service, the Secret Intelligence Service, the Government Communications Headquarters and the Ministry of Defence). During 2015, the Commissioner carried out two such formal inspections of each agency. The Commissioner also conducted inspections of the Home Office, the Foreign Office and the Northern Ireland Office, the departments responsible for processing warrants for each Secretary of State.

The total number of warrants and authorisations approved across the security and intelligence agencies and MoD in 2015 was 1,560. The Commissioner individually scrutinised 499 warrants and authorisations, and their associated paperwork. Of the warrants and authorisations issued during 2015, as distinct from extant at the end of the year, 31% were for Directed Surveillance authorisations, 28% for covert human intelligence source (CHIS) authorisations, 21% for Section 5 authorisations, 12% combined property and intrusive surveillance warrants, 7% for Section 7 authorisations and 1% intrusive surveillance warrants.

⁴² The Commissioner's annual reports can be found in full at intelligencecommissioner.com

An important aspect of the Commissioner's role is to examine errors that occur during the process of the application and authorisation of warrants, or during their subsequent implementation. The Commissioner examines errors in two ways: firstly, through the scrutiny of individual warrants and authorisations as part of his inspection regime; secondly, the agencies are required to report to the Commissioner any error that has resulted in any unauthorised activity where an authorisation should have been in place. Where the agencies are reporting errors to the Commissioner, he expects the reports to explain: when an error occurred; when it was discovered; the nature of the error; how it happened; and what, if any, unauthorised invasion of privacy resulted. The reports also include details of the steps taken to avoid errors happening again.

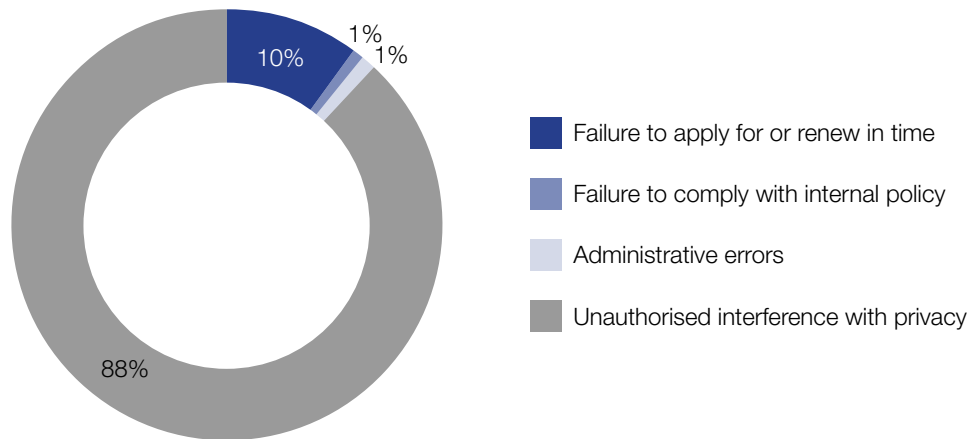
In his Annual Report for 2015, the Commissioner reviewed the categories of error reporting and clarified what is required from the security and intelligence agencies and the MoD. Category A errors are administrative errors; an obvious "slip" where no unauthorised intrusion into privacy had taken place as a result of the slip. These should be reported to the Commissioner in writing bi-annually at inspection. Category B errors are those which are discovered to have occurred inadvertently during a warrant application, authorisation or during the operation of the warrant. These could be, for example, where an agency has operated under a lapsed authorisation, or operated outside the parameters set out in the authorisation in the mistaken belief that it was authorised. These errors should be reported to the Commissioner within three months of the date the error was discovered. Category C errors would be a deliberate decision taken to obtain information without proper authorisation or in any way to act irresponsibly. Such errors should be reported immediately to the Commissioner. If such a deliberate act were to be committed, those involved would be subject to disciplinary action and possible criminal charges.

During 2015, there were 83 errors, compared to 43 errors in 2014. Of this total, 82 were Category B errors or inadvertent errors and only one was a category A or administrative error. There were no Category C errors, as was the case in 2014.

Of the security and intelligence agencies, MI5 reported 67 errors to the Commissioner during 2015. The Commissioner notes that MI5 obtain a larger number of warrants and authorisations than the other agencies and that their error rate is low as a proportion of authorisations. SIS reported 11 errors to the Commissioner during 2015 and GCHQ reported three. The Commissioner did not discover any additional errors during his inspections of these agencies.

In relation to warrant granting departments, one administrative error was brought to the Commissioner's attention when inspecting the Home Office, and the MoD reported one error to the Commissioner during an inspection.

Of the 83 errors reported the most common error was the result of an unauthorised interference with privacy. The breakdown of the causes of these errors is outlined below.

Figure 8: Breakdown of error by cause

Over the year, the Commissioner made 143 recommendations to the Security Service, SIS, GCHQ, MoD, Home Office, Foreign Office and the Northern Ireland Office relating to a range of processes, procedures and guidance available to staff. The Commissioner made a number of specific references to inadequacies in the way SIS record their decision-making in general, but noted improvements regarding the use of the Consolidated Guidance.

During 2015, the Consolidated Guidance was considered on 442 occasions. The Commissioner reviewed 68 of those cases. He was satisfied that the agencies and the MoD took all steps they could to make their personnel aware of the terms of the guidance, and it was clear that careful consideration was given to its application in increasingly complex situations.

The Commissioner's overall conclusion in his 2015 report is that *"authorisations and warrants are only granted on the basis of a proper case for necessity and proper consideration of proportionality. It was evident that the agencies, MoD and Ministers together with their officials all took compliance seriously and put a great deal of effort into ensuring that each interference with privacy was fully justified"*.⁴³

In addition supplementary to his Annual Report, the Commissioner published a report on 15 September 2016 on his investigation into concerns raised by the Intelligence and Security Committee of Parliament in their report on the murder of Fusilier Lee Rigby.⁴⁴ In their report, the ISC were critical of SIS for their handling of allegations of Michael Adebolajo's mistreatment in Kenya made during his interview by police under the Terrorism Act 2000 on his return to the UK. Following his investigation, the Commissioner concluded that Mr Adebolajo was not the victim of a conspiracy, torture or mistreatment, and that the response of the Security Service (MI5) and SIS to the arrest and detention was generally

43 "Report of the Intelligence Services Commissioner for 2015", page 65.

44 This report can be accessed at intelligencecommissioner.com

good. However, the Commissioner considered that there were some inadequacies in the responses of a number of government departments to the allegations of mistreatment and in the manner in which SIS engaged with the investigation. The Commissioner set out a number of recommendations based on his conclusions, including a proposal that the Government produce and adopt a protocol for improving engagement with security and intelligence oversight investigations.

The Government welcomed this report, the Commissioner's detailed examination of the allegations, and his rejection of any suggestion of a conspiracy by the security and intelligence agencies in Mr Adebolajo's detention. In a written statement to both Houses of Parliament on 15 September 2016, the Prime Minister stated that *'the Government will look carefully at Sir Mark's detailed analysis of the handling of this case and will take steps to address the issues where he has identified shortcomings in the response at the time, drawing upon the report's recommendations'*.

7.4 – Office of Surveillance Commissioners

The Office of Surveillance Commissioners is responsible for providing robust, independent oversight of the use of covert surveillance powers by public authorities, excluding the security and intelligence agencies. The Chief Surveillance Commissioner, The Rt Hon the Lord Judge, and the Surveillance Commissioners, were appointed by the Prime Minister under section 91 of the Police Act 1997. All Commissioners are required to hold, or have held, high judicial office in order to be appointed to their roles.

The statutory responsibilities of the Chief Surveillance Commissioner are drawn from the Police Act 1997, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A). His specific responsibilities are to oversee:

- the performance of functions under Part III of the Police Act 1997 (PA 97);
- except in relation to the security and intelligence agencies, the exercise and performance of the powers and duties conferred by or under Parts II and III of RIPA; and
- the exercise and performance of the powers and duties conferred or imposed by or under RIP(S)A.

The Chief Surveillance Commissioner also acts as the Investigatory Powers Commissioner for the Sovereign Base Areas, Cyprus, under the Regulation of Investigatory Powers Ordinance 2012.

There are six Surveillance Commissioners working under the Chief Surveillance Commissioner. These six Commissioners have statutory responsibilities to undertake the following activities:

- grant prior approval for authorisations and renewals of any intrusive surveillance;

- grant prior approval for property interference where it involves a hotel bedroom, a dwelling, or office premises, or where it might involve the acquisition of matters subject to legal privilege, confidential personal information or journalistic material;
- grant prior approval for any CHIS whose activities will result in the CHIS obtaining, providing access to or disclosing matters subject to legal privilege;
- grant prior approval for the renewal of law enforcement “relevant sources” (commonly termed undercover officers);
- note all other property interference authorisations, renewals and cancellations, and “relevant source” authorisations and cancellations;
- assist the Chief Surveillance Commissioner in his oversight of notification of disclosure requirement notices served in respect of electronic information protected by encryption; and
- assist the Chief Surveillance Commissioner in his duty to keep under review the use of directed surveillance and CHIS by law enforcement agencies.

The Commissioners will only grant prior approval for any authorisation or renewal where the relevant action is necessary and proportionate. Where, at any time, a Commissioner is satisfied that there are not reasonable grounds for believing that an action is necessary and proportionate, he/she may quash an authorisation or renewal.

In addition to the six Commissioners, the Office of Surveillance Commissioners also includes three Assistant Surveillance Commissioners and a number of Inspectors. The primary responsibility of the Assistant Commissioners is to oversee the activities of public authorities that are not law enforcement agencies, such as local authorities, in the exercise of their powers under Part II of RIPA. To be appointed as an Assistant Surveillance Commissioner, an individual must hold, or have held, office as a judge of the Crown Court, a Circuit judge, a sheriff in Scotland, or a county court judge in Northern Ireland. The Surveillance Inspectors are responsible for assisting the Chief Surveillance Commissioner by undertaking detailed inspections of the public authorities whose activities he is tasked to oversee.

The Chief Surveillance Commissioner reports annually to the Prime Minister and to Scottish Ministers on the matters for which he is responsible under the Police Act 1997, RIPA and RIP(S)A. These reports are presented to Parliament and laid before the Scottish Parliament, and are publically available. The Chief Surveillance Commissioner’s most recent report was laid before Parliament on 7 July 2016 and covers the period 1 April 2015 to 31 March 2016.⁴⁵ Alongside the report, the Commissioner made public, for the first time, the Office of Surveillance Commissioners’ Procedures & Guidance document.⁴⁶ Access to this guidance had been limited to those working within public authorities empowered to use covert surveillance, but is now in the public domain. It provides a wider perspective of the circumstances in which covert surveillance is authorised and supervised. This Guidance does not replace the legislative provisions or the associated Codes of Practice.

45 The Commissioner’s annual reports can be found in full at <https://osc.independent.gov.uk/>

46 <https://osc.independent.gov.uk/wp-content/uploads/2017/01/OSC-Procedures-Guidance-July-2016.pdf>

The Commissioner’s annual report includes statistics on the use of the powers of which he has oversight. Further details are included in Chapter 6 of this report.

The Commissioner’s annual report includes details of the number of irregularities reported to him during the reporting period. For law enforcement agencies, there were 96 irregularities reported to the Commissioner and for other public authorities, there were four. The Commissioner outlines that the nature of irregularities varies very little from year to year. There were instances of pre-emptive activity before the authorisation had been granted resulting from misunderstanding or poorly completed checks, overdue switching off of a recording device once an authorisation had been cancelled, and the use of a CHIS without an authorisation for use and conduct. The report highlights very minor errors, such as a small error in the positioning of a camera, the use of which has otherwise been properly authorised or activity undertaken, usually in the heat of the moment by a quick thinking, but untrained or inexperienced police officer.⁴⁷

The Commissioner is clear that there is nothing to suggest wilful misconduct or bad faith in relation to any of these irregularities and that a total of 100 irregularities is an extremely small proportion of the total number of authorisations. The Commissioner reported that the overwhelming majority are the result of human error, which reinforces the need for regular training and continued robust oversight by senior officers and managers of the processes. The Commissioner further recommended that every authority vested with the relevant statutory powers should have in place structures and training arrangements to ensure that the exercise of any such powers will be lawful.

The Government welcomed the Commissioner’s report and his conclusion that: *“the powers created by the legislation are exercised with great circumspection, following careful analysis of whether and what form of covert surveillance is both ‘necessary’ and ‘proportionate’ and, with appropriate caution, where, collaterally, it may impact on those against whom there are no grounds for suspecting serious criminal conduct. I believe that the system of checks and balances is working well.”*

7.5 – Investigatory Powers Tribunal

The Investigatory Powers Tribunal (IPT) was established in October 2000 under Part IV of the RIPA. It is one part of a range of oversight provisions that ensure public authorities act in a way that is compatible with the Human Rights Act 1998.

The IPT is independent of Government and ensures that members of the public have an effective right of redress if they believe they have been a victim of unlawful action under RIPA, or wider human rights infringements in breach of the Human Rights Act 1998. Members of the IPT must be senior members of the legal profession and both the president and vice president must have held high judicial office. There are currently eight members of the IPT. The President is Sir Michael Burton and the Vice President is Mr Justice Mitting.

47 “Annual Report of the Chief Surveillance Commissioner for 2015-2016”, paragraph 4.17, page 17.

The Tribunal was established to consider, and if necessary, investigate and determine, any complaints made by members of the public (including non-governmental organisations) which fall into the following two categories.

First, the Tribunal can consider any complaint by a person who believes that he or she has been the victim of unlawful interference by public authorities, including the military, law enforcement and the security and intelligence agencies, using the investigatory powers regulated under RIPA. A complaint can be about any interference which the complainant believes has taken place against him, his property or communications, and can relate to interception, communications data acquisition, surveillance and property interference.

Second, the Tribunal also considers complaints where the claimant alleges they have been the victim of a human rights violation relating to the use of covert techniques by the military, law enforcement or the security and intelligence agencies, as well as a wider range of human rights breaches believed to have been committed by the security and intelligence agencies.

Members of the public are free to make the first type of complaint (interference by public authorities) to the ordinary courts instead of the Tribunal, but the Tribunal has additional powers of investigation which a court does not have. In cases of human rights breaches involving the security and intelligence agencies, the Tribunal is the only forum that can decide the complaint.

IPT Statistics

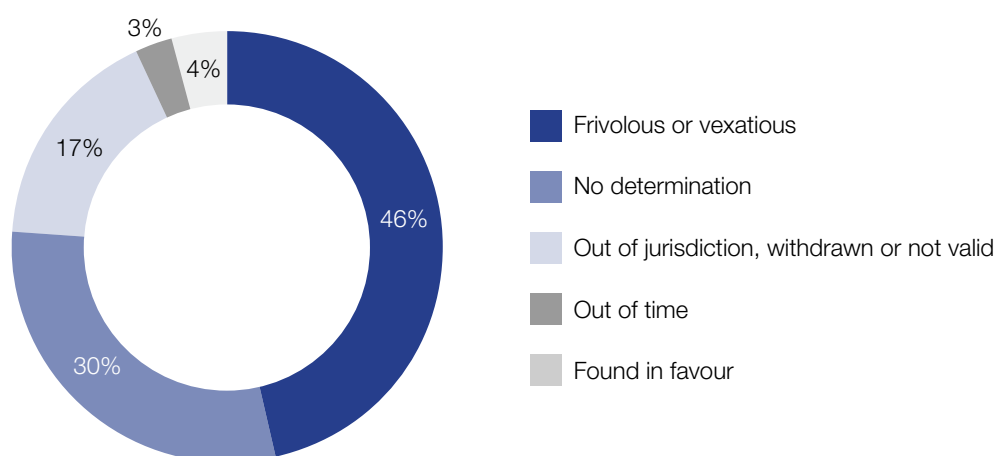
In July 2016, the Tribunal released a report covering the period 1 January 2011 to 31 December 2015, which also included a number of notable cases from spring 2016. The report highlighted that the number of complaints received by the Tribunal has increased steadily since its inception. The volume of complaints to the Tribunal has risen from 95 in its first year to over 250 in the last full year of this report.

The report indicated that this increase may be in part due to the Snowden leaks in 2013, but also to cases being brought by non-governmental organisations NGOs, more power being held by public authorities, amendments to RIPA that have widened the jurisdiction of the Tribunal, and members of the public becoming increasingly aware of the Tribunal as a legal recourse.

During 2015, the IPT received 251 new cases and decided 219 cases. Out of these 219 cases, 101 (47%) were ruled to be frivolous or vexatious. These cases are ones where the allegation or belief is so fanciful that it is considered not to be sustainable. The decision to assess a case as frivolous or vexatious is always taken by at least two Tribunal Members. In 65 (30%) of the cases, there was a “no determination outcome”. This means that the Tribunal ruled there was no unlawful or unreasonable activity involving the complainant. 38 (17%) cases were ruled to be out of the Tribunal’s jurisdiction, or were either withdrawn or invalid. Seven (3%) cases were ruled to be out of time and in eight (4%) cases, the Tribunal found in favour of the complainant.

Full copies of the Tribunal’s judgments are available on the Tribunal website at www.ipt-uk.com.

Figure 9: Outcomes of cases decided at the IPT, 2015



Details of all of the cases received and decided by the IPT between 2011 and 2015 are at Annex D.⁴⁸

⁴⁸ All of the Tribunal judgements arising from oral hearings are published on the Tribunal website at www.ipt-uk.com and BAILI (The British and Irish Legal Information Institute).



8 – Recommended Reading List

Legislation

- Anti-social Behaviour, Crime and Policing Act 2014 – www.legislation.gov.uk/ukpga/2014/12/contents
- Counter-Terrorism and Security Act 2015 – www.legislation.gov.uk/ukpga/2015/6/contents
- Data Protection Act 1998 – www.legislation.gov.uk/ukpga/1998/29/contents
- Data Retention and Investigatory Powers Act 2014 – www.legislation.gov.uk/ukpga/2014/27/contents
- Data Retention Regulations 2014 – www.legislation.gov.uk/uksi/2014/2042/contents/made
- Digital Economy Bill 2016-2017 – <https://services.parliament.uk/bills/2016-17/digitaleconomy.html>
- Freedom of Information Act 2000 – www.legislation.gov.uk/ukpga/2000/36/contents
- Human Rights Act 1998 – www.legislation.gov.uk/ukpga/1998/42/contents
- Intelligence Services Act 1994 – www.legislation.gov.uk/ukpga/1994/13/contents
- Investigatory Powers Act 2016 – <http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted>
- Justice and Security Act 2013 – www.legislation.gov.uk/ukpga/2013/18/contents
- Police Act 1997 – www.legislation.gov.uk/ukpga/1997/50/contents
- Policing and Crime Bill 2015-2017 – <http://services.parliament.uk/bills/2016-17/policingandcrime.html>
- Privacy and Electronic Communications (EC Directive) Regulations 2003 – www.legislation.gov.uk/uksi/2003/2426/contents/made
- Proscribed Organisations (Applications for Deproscription etc) Regulations 2006 (SI 2006/2299) – www.legislation.gov.uk/uksi/2006/2299/made
- Protection of Freedoms Act 2012 – www.legislation.gov.uk/ukpga/2012/9/contents
- Regulation of Investigatory Powers Act 2000 – www.legislation.gov.uk/ukpga/2000/23/contents
- Terrorism Act 2000 – www.legislation.gov.uk/ukpga/2000/11/contents

- Terrorism Act 2006 – www.legislation.gov.uk/ukpga/2006/11/contents
- Terrorist Asset-Freezing etc Act 2010 – www.legislation.gov.uk/ukpga/2010/38/contents
- Terrorism Prevention and Investigation Measures Act 2011 – www.legislation.gov.uk/ukpga/2011/23

Government Publications

- CONTEST: The United Kingdom's Strategy for Countering Terrorism – www.gov.uk/government/collections/contest
- CONTEST Annual Report for 2015 – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/539683/55469_Cm_9310_Web_Accessible_v0.11.pdf
- Counter-Terrorism Statistics, Operation of Police Powers under the Terrorism Act 2000 – <https://www.gov.uk/government/collections/counter-terrorism-statistics>
- HM Government Modern Crime Prevention Strategy – <https://www.gov.uk/government/publications/modern-crime-prevention-strategy>
- National Crime Agency annual report and accounts 2015 to 2016 – <https://www.gov.uk/government/publications/national-crime-agency-annual-report-and-accounts-2015-to-2016>
- Statistics on Closed Material Procedure – <https://www.gov.uk/government/publications/use-of-closed-material-procedure-report-25-june-2015-to-24-june-2016>
- Statistics on Terrorist Asset-Freezing – <https://www.gov.uk/government/collections/operation-of-the-uks-counter-terrorist-asset-freezing-regime-quarterly-report-to-parliament>

Independent Publications

- Bulk Powers Review by the Independent Reviewer of Terrorism – <https://terrorismlegislationreviewer.independent.gov.uk/bulk-powers-review-report/>
- A Question of Trust: Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation – <https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/>
- Chief Surveillance Commissioner, Annual Report 2015/2016 – <https://osc.independent.gov.uk/wp-content/uploads/2016/07/OSC-Annual-Report-2015-2016-2.pdf>

- Independent Reviewer of Terrorism Legislation, Annual Reports (Terrorism Acts, TPIMs, Asset-Freezing) –
<https://terrorismlegislationreviewer.independent.gov.uk/category/reports>
- Intelligence and Security Committee, Report on Privacy and Security –
[http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt\(web\).pdf](http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf)
- Intelligence Service Commissioner, Annual Report for 2015 –
<http://intelligencecommissioner.com/docs/56892%20HC%20459%20web.pdf>
- Interception of Communications Commissioner, Annual Report 2015 –
<http://www.iocco-uk.info/docs/56850%20HC%20255%20ICCO%20Web%20only.pdf>
- Interception of Communications Commissioner section 94 report –
<http://www.iocco-uk.info/docs/56208%20HC33%20WEB.pdf>
- Investigatory Powers Tribunal, Case Statistics and Judgments – www.ipt-uk.com
- Royal United Services Institute, Independent Surveillance Review – www.rusi.org



9 – Annexes

ANNEX A – Terrorist Asset-Freezing Figures, 1 July 2016 – 30 September 2016

| | Tafa 2010 | EU Reg(EC) 2580/2001 | Al-Qaida regime UNSCR 1989 |
|----------------------------------------------------------------------------|-----------|-------------------------|-------------------------------|
| Assets frozen (as at 30/09/2016) | £9,000 | £0 | £66,000 ⁴⁵ |
| Number of accounts frozen in UK (at 30/09/2016) | 6 | 1 | 34 |
| New accounts frozen (during Q3 2016) | 0 | 0 | 0 |
| Accounts unfrozen (during Q3 2016) | 29 | 0 | 0 |
| Total number of designations (at 30/09/2016) | 21 | 32 | 337 |
| Number of designations that were confidential | 0 | N/A | N/A |
| (i) New designations (during Q3 2016, including confidential designations) | 0 | 0 | 2 |
| (ii) Delistings (during Q3 2016) | 2 | 0 | 2 |
| (iii) Individuals in custody in UK (at 30/09/2016) | 0 | 0 | 0 |
| (iv) Individuals in UK, not in custody (at 30/09/2016) | 0 | 0 | 2 |
| (v) Individuals overseas (at 30/09/2016) | 14 | 10 | 260 |
| (vi) Groups | 7 | 22 | 75 |

49 This figure reflects the most up-to-date account balances available and includes some funds denominated in dollars that are frozen in the UK. This has been converted using exchange rates as of 30/09/2016. Additionally, the figures reflect an updating of balances of accounts for certain individuals during the quarter, depleted through licensed activity.

| | TAFAs 2010 | EU Reg(EC) 2580/2001 | Al-Qaida regime UNSCR 1989 |
|--------------------------------------------|-------------------|---------------------------------|---------------------------------------|
| Individuals by Nationality | | | |
| (i) UK Nationals ⁴⁶ | 0 | n/a | n/a |
| (ii) Non UK Nationals | 14 | | |
| Renewal of designation (during Q3 2016) | 5 | n/a | n/a |
| General Licences | | | |
| (i) Issued in Q2 | (i) 0 | | |
| (ii) Amended | (i) 0 | | |
| (iii) Revoked | (i) 1 | | |
| Specific Licences: | | | |
| (i) Issued in Q3 | 15 | 0 | 0 |
| (ii) Amended | 0 | 0 | 0 |
| (iii) Expired | 0 | 0 | 0 |
| (iv) Revoked/Redundant | 22 | 0 | 0 |
| (v) Refused | 0 | 0 | 0 |

50 Based on information held by the Treasury, some of these individuals hold dual nationality.

ANNEX B – Proscribed Organisations

- 71 international terrorist organisations are proscribed under the Terrorism Act 2000.
- 14 organisations in Northern Ireland were proscribed under previous legislation.

The information about the groups' aims was given to Parliament when they were proscribed.

Users should bear in mind that there is no universal standard for transliterating Arabic and other languages into Latin characters. Therefore, the spelling of the names of proscribed organisations appearing in other publications may differ slightly from that given in this list.

17 November Revolutionary Organisation (N17) – Proscribed March 2001

Aims to highlight and protest at what it deems to be imperialist and corrupt actions, using violence. Formed in 1974 to oppose the Greek military Junta, its stance was initially anti-Junta and anti-US, which it blamed for supporting the Junta.

Abdallah Azzam Brigades, including the Ziyad al-Jarrah Battalions (AAB) – Proscribed June 2014

AAB is an Islamist militant group aligned with Al Qa'ida and the global jihad movement, currently fighting in Syria and Lebanon. The group began operating in Pakistan in 2009. The Lebanese branch uses the name the Ziyad al Jarrah Battalion, and is named after Lebanese 9/11 hijacker Ziyad al Jarrah who participated in the hijacking and crash of United Flight 93.

AAB has increased its operational pace since the onset of the Syrian insurgency, claiming responsibility for a rocket attack launched from Lebanon into northern Israel in August 2013. On 19 November 2013, AAB claimed responsibility for a double suicide bombing outside the Iranian embassy in Beirut, which killed at least 22 people and wounded over 140.

On 19 February 2014, the group's media wing, the Al-Awzaey Media Foundation, announced on Twitter and YouTube that the group claimed responsibility for two suicide bombings near the Iranian cultural centre in Beirut killing 11 and wounding 130, in revenge for actions by Iran and Hizballah, in Lebanon and Syria.

The group has threatened to launch further terrorist attacks and has demanded that the Lebanese Government free imprisoned jihadists. It has also threatened attacks on Western targets in the Middle East.

Abu Nidal Organisation (ANO) – Proscribed March 2001

ANO's principal aim is the destruction of the state of Israel. It is also hostile to 'reactionary' Arab regimes and states supporting Israel.

Abu Sayyaf Group (ASG) – *Proscribed March 2001*

The precise aims of the ASG are unclear, but its objectives appear to include the establishment of an autonomous Islamic state in the Southern Philippine island of Mindanao.

Ajnad Misr (Soldiers of Egypt) – *Proscribed November 2014*

The group is a jihadist group based in Egypt and is believed to be a splinter group of Ansar Bayt al Maqdis (ABM), which was proscribed on 4 April. Ajnad Misr has stated that it seeks to protect Egyptian Muslims and avenge alleged abuse against them by the Egyptian security services.

Ajnad Misr is believed to have been active since 20 November 2013, when it attacked an Egyptian checkpoint. It announced its establishment on 23 January 2014 and has claimed responsibility a number of attacks on Egyptian security forces in a military campaign. The claims were made in three communiqués posted on its Facebook and Twitter accounts on 23 January, 24 January, and 31 January. On the jihadi forum al-Fida', Ansar Bayt al Maqdis, referred to Ajnad Misr in a communiqué issued on January 28, expressing support for the group and identifying it as being responsible for two attacks in Greater Cairo in January. Ajnad Misr has claimed responsibility for the bombing at Cairo University on 2 April that resulted in the death of a policeman and injuries to three others.

Al-Gama'at al-Islamiya (GI) – *Proscribed March 2001*

The main aim of GI is to overthrow the Egyptian government and replace it with an Islamic state through all means, including the use of violence. Some members also want the removal of Western influence from the Arab world.

Al Ghurabaa – *Proscribed July 2006*

Al Ghurabaa / The Saved Sect is an Islamist group which seeks to establish an Islamic Caliphate ruled by Shariah law. The group first emerged as Al Muhajiroun in the UK, in 1996, led by Omar Bakri Muhammed, who then publicly disbanded the organisation in 2004. The organisation reformed in 2004 under the names Al Ghurabaa and the Saved Sect. While the Group has some links to groups overseas, it is based and operates within the UK.

Note: The Government laid Orders, in January 2010 and November 2011, which provide that **Al Muhajiroun, Islam4UK, Call to Submission, Islamic Path, London School of Sharia** and **Muslims Against Crusades** should be treated as alternative names for the organisation which is already proscribed under the names Al Ghurabaa and **The Saved Sect**.

The Government laid an Order, in June 2014 recognising **Need4Khilafah, the Shariah Project** and the **Islamic Dawah Association** as the same as the organisation proscribed as Al Ghurabaa and The Saved Sect, which is also known as Al Muhajiroun.

Al Ittihad Al Islamia (AIAI) – Proscribed October 2005

The main aims of AIAI are to establish a radical Sunni Islamic state in Somalia, and to regain the Ogaden region of Ethiopia as Somali territory via an insurgent campaign. Militant elements within AIAI are suspected of having aligned themselves with the ‘global jihad’ ideology of Al Qa’ida, and to have operated in support of Al Qa’ida in the East Africa region.

Al Murabitun – Proscribed April 2014

Al Murabitun resulted from a merger of two Al Qa’ida in the Maghreb (AQ-M) splinter groups that are active in Mali and Algeria, the Movement for the Unity and Jihad in West Africa (MUJWA) and Mokhtar Belmokhtar’s group, the Al Mulathamine Battalion which included the commando element ‘Those Who Sign in Blood’. The merger was announced in a public statement in August 2013.

Al Murabitun aspires to unite Muslims from “the Nile to the Atlantic” and has affirmed its loyalty to al-Qaida leader Ayman al-Zawahiri and the emir of the Afghan Taleban, Mullah Omar.

As at 3 April 2014, the group has not claimed responsibility for any terrorist attacks since the merger but both precursor groups have participated in a number of terrorist attacks and kidnapping for ransom during the past 13 months. Belmokhtar’s group was responsible for the attack against the In Amenas gas facility in January 2013 that resulted in the death of over thirty people including Britons. In May 2013 the two groups targeted a military barracks in Agadez, Niger and a uranium mine in Arlit which supplies French nuclear reactors. The suicide attack in Agadez resulted in the deaths of at least twenty people.

Despite previously separating themselves from AQM, citing leadership issues and the desire to expand their control, both precursor groups continued to cooperate and fight alongside AQM fighters in Mali and other regions of West Africa. This activity has continued since the merger.

Al Qa’ida (AQ) – Proscribed March 2001

Inspired and led by Usama Bin Laden, its aims are the expulsion of Western forces from Saudi Arabia, the destruction of Israel and the end of Western influence in the Muslim world.

Note: The Government laid an Orders, in July 2013 and December 2016, which provided that the **al-Nusra Front (ANF)**, **Jabhat al-Nusra li-ahl al Sham** and **Jabhat Fatah al-Sham** should be treated as alternative names for the organisation which is already proscribed under the name Al Qa’ida.

Al Shabaab – Proscribed March 2010

Al Shabaab is an organisation based in Somalia which has waged a violent campaign against the Somali Transitional Federal Government and African Union peacekeeping forces since 2007, employing a range of terrorist tactics including suicide bombings, indiscriminate attacks and assassinations. Its principal aim is the establishment of a fundamentalist Islamic state in Somalia, but the organisation has publicly pledged its allegiance to Usama Bin Laden and has announced an intention to combine its campaign in the Horn of Africa with Al Qa'ida's aims of global jihad.

Ansar Al Islam (AI) – Proscribed October 2005

AI is a radical Sunni Salafi group from northeast Iraq around Halabja. The group is anti-Western, and opposes the influence of the US in Iraqi Kurdistan and the relationship of the KDP and PUK to Washington. AI has been involved in operations against Multi-National Forces-Iraq (MNF-I).

Ansar al-Sharia-Benghazi (AAS-B) which translates as the Partisans of Islamic Law – Proscribed November 2014

AAS-B is a Sunni Islamist militia group that has an anti-Western rhetoric and advocates the implementation of strict Sharia law. AAS-B came into being in 2011, after the fall of the Gaddafi regime. The group was led by Mohammed Ali al-Zahawi and Ahmed Abu Khattalah is an AAS-B senior leader.

AAS-B is involved in terrorist attacks against civilian targets, frequent assassinations, and attempted assassinations of security officials and political actors in eastern Libya. On 11 September, 2012 members of AAS-B took part in the attack against the U.S. Special Mission and Annex in Benghazi, Libya, killing the US ambassador and three other Americans. In September 2012, Mohammed Ali al-Zahawi, in an interview openly stated his support for Al Qa'ida's strategy but denied any links to the organisation. He also confirmed AAS-B had demolished and desecrated Sufi shrines in Benghazi, which the group regard as idolatrous.

AAS-B used its online presence to denounce the 2013 capture and removal from Libya of al Qa'ida operative Abu Anas al-Libi, by American military forces. In August 2013, Ahmed Abu Khattala, a senior leader of the group, was charged with playing a significant role in last year's attack on the U.S. diplomatic compound in Benghazi.

AAS-B continues to pose a threat to Libya and Western interests and is alleged to have links to proscribed organisation Ansar al-Sharia-Tunisia and Al Qa'ida.

The US designated AAS-B as a terrorist organisation in January 2014 and the UN listed AAS-B on 19 November.

Ansar Al Sharia-Tunisia (AAS-T) – Proscribed April 2014

Ansar Al Sharia-Tunisia (AAS-T) is a radical Islamist group founded in April 2011. The group aims to establish Sharia law in Tunisia and eliminate Western influence. The group is ideologically aligned to Al Qa'ida (AQ) and has links to AQ affiliated groups. It is reported that the group announced its loyalty to AQM in September 2013.

AAS-T's leader, Seif Allah Ibn Hussein also known as Abu Ayadh al-Tunis, is a former AQ veteran combatant in Afghanistan. He has been hiding following issue of a warrant for his arrest relating to an allegation of inciting the attack on the US Embassy in Tunis that killed four people in September 2012.

Extremists believed to have links with AAS-T are assessed to be responsible for the attacks in October 2011 on a television station and, in June 2012, an attack on an art exhibit. AAS-T is assessed to be responsible for the attacks on the US Embassy and American school in Tunis in September 2012. The Tunisian government believe AAS-T was responsible for the assassination of two National Coalition Assembly members; Chokri Belaid in February 2013 and Mohamed Brahmi in July 2013.

Additionally, elements of the group are believed to have been involved in the attempted suicide attack, in October 2013, at a hotel in a tourist resort in Sousse where a significant number of British tourists were staying.

Ansar Al Sunna (AS) – Proscribed October 2005

AS is a fundamentalist Sunni Islamist extremist group based in central Iraq and what was the Kurdish Autonomous Zone (KAZ) of Northern Iraq. The group aims to expel all foreign influences from Iraq and create a fundamentalist Islamic state.

Ansar Bayt al-Maqdis (ABM) – Proscribed April 2014

ABM is an Al Qa'ida inspired militant Islamist group based in the northern Sinai region of Egypt. The group is said to recruit within Egypt and abroad and aims to create an Egyptian state ruled by Sharia law.

ABM is assessed to be responsible for a number of attacks on security forces in Egypt since 2011. The attacks appear to have increased since the overthrow of the Morsi government in July 2013. The group's reach goes beyond the Sinai, with the group claiming responsibility for a number of attacks in Cairo and cross-border attacks against Israel. ABM has undertaken attacks using vehicle borne improvised explosive devices and surface-to-air missiles. Examples of attacks that the group has claimed responsibility for include:

- in September 2013 an attack on the Egyptian Interior Minister in which a UK national was seriously injured;
- the attack on a police compound in Mansoura on 24 December 2013, killing at least 16 people, including 14 police officers; and

- an attack on a tourist bus in which three South Koreans and their Egyptian driver died on 16 January 2014.

Ansarul Muslimina Fi Biladis Sudan (Vanguard for the protection of Muslims in Black Africa) (Ansaru) – Proscribed November 2012

Ansaru is an Islamist terrorist organisation based in Nigeria. They emerged in 2012 and are motivated by an anti-Nigerian Government and anti-Western agenda. They are broadly aligned with Al Qa'ida.

Armed Islamic Group (Groupe Islamique Armée) (GIA) – Proscribed March 2001

The aim of the GIA is to create an Islamic state in Algeria using all necessary means, including violence.

Asbat Al-Ansar ('League of Partisans' or 'Band of Helpers') – Proscribed November 2002

Sometimes going by the aliases of 'The Abu Muhjin' group/faction or the 'Jama'at Nour', this group aims to enforce its extremist interpretation of Islamic law within Lebanon and, increasingly, further afield.

Babbar Khalsa (BK) – Proscribed March 2001

BK is a Sikh movement that aims to establish an independent Khalistan within the Punjab region of India.

Basque Homeland and Liberty (Euskadi ta Askatasuna) (ETA) – Proscribed March 2001

ETA seeks the creation of an independent state comprising the Basque regions of both Spain and France.

Baluchistan Liberation Army (BLA) – Proscribed July 2006

BLA are comprised of tribal groups based in the Baluchistan area of Eastern Pakistan, which aims to establish an independent nation encompassing the Baluch dominated areas of Pakistan, Afghanistan and Iran.

Boko Haram (Jama'atu Ahli Sunna Lidda Awati Wal Jihad) (BH) – Proscribed July 2013

Boko Haram is a terrorist organisation, based in Nigeria that aspires to establish Islamic law in Nigeria and has carried out a number of terrorist attacks that have targeted all sections of Nigerian society.

Egyptian Islamic Jihad (EIJ) – Proscribed March 2001

The main aim of the EIJ is to overthrow the Egyptian government and replace it with an Islamic state. However, since September 1998, the leadership of the group has also allied itself to the ‘global Jihad’ ideology expounded by Usama Bin Laden and has threatened Western interests.

Global Islamic Media Front (GIMF) including GIMF Bangla Team (also known as Ansarullah Bangla Team (ABT) and Ansar-al Islam) – Proscribed July 2016

GIMF is an Islamist extremist propaganda organisation associated with Al Qa’ida (AQ) and other extremist groups around the world. Its activities include propagating a jihadist ideology, producing and disseminating training manuals to guide terror attacks and publishing jihadi news casts. GIMF releases products in a number of languages including Arabic, Urdu, Bengali, English, German and French.

On 31 December 2015, the GIMF announced the merger of ABT into its ranks, renaming it GIMF Bangla Team. Prior to the merger, using the names ABT and Ansar-al Islam, the group claimed responsibility for the prominent murders and attacks of secular bloggers from 2013 to 2015: including Bangladeshi-American Avijit Roy; Niladri Chatterji Niloy; Ahmed Rajib Haider; Asif Mohiuddin; Oyasiqur Rahman; Ananta Bijoy; Das and AKM Shafiu Islam. The group have been linked to a number of hit lists of bloggers, writers and activists around the world (including nine individuals based in Britain, seven in Germany and two in America, one in Canada and one in Sweden) in 2015.

On 7 January 2016 GIMF Bangla Team published an infographic chronicling attacks carried out against “blasphemers in Bangladesh” from January 2013 to October 2015. The graphic contained names and locations of 13 attacks, eight of which were celebrated as successful assassinations. Bangladesh banned ABT in May 2015.

Groupe Islamique Combattant Marocain (GICM) – Proscribed October 2005

The traditional primary objective of the GICM has been the installation of a governing system of the caliphate to replace the governing Moroccan monarchy. The group also has an Al Qa’ida-inspired global extremist agenda.

Hamas Izz al-Din al-Qassem Brigades – Proscribed March 2001

Hamas aims to end Israeli occupation in Palestine and establish an Islamic state.

Harakat-UI-Jihad-UI-Islami (HUJI) – Proscribed October 2005

The aim of HUJI is to achieve through violent means accession of Kashmir to Pakistan, and to spread terror throughout India. HUJI has targeted Indian security positions in Kashmir and conducted operations in India proper.

Harakat-UI-Jihad-UI-Islami (Bangladesh) (HUJI-B) – Proscribed October 2005

The main aim of HUJI-B is the creation of an Islamic regime in Bangladesh modelled on the former Taliban regime in Afghanistan.

Harakat-UI-Mujahideen/Alami (HuM/A) and Jundallah – Proscribed October 2005

The aim of both HuM/A and Jundallah is the rejection of democracy of even the most Islamic-oriented style, and to establish a caliphate based on Sharia law, in addition to achieving accession of all Kashmir to Pakistan. HuM/A has a broad anti-Western and anti-President Musharraf agenda.

Harakat Mujahideen (HM) – Proscribed March 2001

HM, previously known as Harakat UI Ansar (HuA) seeks independence for Indian-administered Kashmir. The HM leadership was also a signatory to Usama Bin Laden's 1998 fatwa, which called for worldwide attacks against US and Western interests.

Haqqani Network (HQN) – Proscribed March 2015

The Haqqani Network (HQN) is an Islamist, nationalist group seeking to establish sharia law and control territory in Afghanistan. It is ideologically aligned with the Taleban, and aims to eradicate Western influence, disrupt the Western military and political efforts in Afghanistan. The group is demanding that US and Coalition Forces withdraw from Afghanistan. The group is led by Jalaluddin Haqqani and his son, Sirajuddin.

HQN has links with a number of terrorist groups in the region including proscribed Central Asian group Islamic Jihad Union (IJU). HQN also have long established links with Al Qa'ida (AQ) that were strengthened after the removal of the Taleban by the US when AQ leader Osama bin Laden was probably sheltered by Jalaluddin in North Waziristan (NWA).

HQN continues to play an active and influential role in the Afghan insurgency in the East of the country and is seeking to expand its influence in to other areas of Afghanistan. While it can be difficult to identify specific HQN responsibility for attacks, given the Taleban practice of claiming attacks on behalf of the insurgency as a whole, the group believed to have been responsible for the recent attack against the British Embassy vehicle in November 2014 which killed six people including a UK national and an Afghan member of UK Embassy staff and injuring more than 30 people.

It is likely that HQN will continue to view Kabul as a key target location due to the concentration of UK and Western interests in the capital.

HQN has been banned as a terrorist group by the USA since September 2012, Canada since May 2013 and the UN since November 2012.

Hizballah Military Wing – *Hizballah's External Security Organisation was proscribed March 2001 and in 2008 the proscription was extended to Hizballah's Military apparatus including the Jihad Council*

Hizballah is committed to armed resistance to the state of Israel, and aims to seize all Palestinian territories and Jerusalem from Israel. Its military wing supports terrorism in Iraq and the Palestinian territories.

Hezb-E Islami Gulbuddin (HIG) – *Proscribed October 2005*

Led by Gulbuddin Hekmatyar who is in particular very anti-American, HIG is anti-Western and desires the creation of a fundamentalist Islamic State in Afghanistan.

Imarat Kavkaz (IK) (also known as the Caucasus Emirate) – *Proscribed December 2013*

Imarat Kavkaz seeks a Sharia-based Caliphate across the North Caucasus. It regularly uses terrorist tactics and has carried out attacks against both Russian state and civilian targets. The organisation claimed responsibility for the attack on Domodedovo airport in Moscow in January 2011, that killed 35 including one British national and a suicide attack on the Moscow Metro in March 2010 that killed 39. Since then there has been continued activity by Imarat Kavkaz, including renewed threats of terrorist activity in Russia.

Indian Mujahideen (IM) – *Proscribed July 2012*

IM aims to establish an Islamic state and implement Sharia law in India using violent means.

Islamic Army of Aden (IAA) – *Proscribed March 2001*

The IAA's aims are the overthrow of the current Yemeni government and the establishment of an Islamic State following Sharia Law.

Islamic Jihad Union (IJU) – *Proscribed July 2005*

The primary strategic goal of the IJU is the elimination of the current Uzbek regime. The IJU would expect that following the removal of President Karimov, elections would occur in which Islamic-democratic political candidates would pursue goals shared by the IJU leadership.

Islamic Movement of Uzbekistan (IMU) – *Proscribed November 2002*

The primary aim of IMU is to establish an Islamic state in the model of the Taliban in Uzbekistan. However, the IMU is reported to also seek to establish a broader state over the entire Turkestan area.

Islamic State of Iraq and the Levant (ISIL) also known as Dawlat al-'Iraq al-Islamiyya, Islamic State of Iraq (ISI), Islamic State of Iraq and Syria (ISIS) and Dawlat al Islamiya fi Iraq wa al Sham (DAISh) and the Islamic State in Iraq and Sham – Proscribed June 2014

ISIL is a brutal Sunni Islamist terrorist group active in Iraq and Syria. The group adheres to a global jihadist ideology, following an extreme interpretation of Islam, which is anti-Western and promotes sectarian violence. ISIL aims to establish an Islamic State governed by Sharia law in the region and impose their rule on people using violence and extortion.

ISIL was previously proscribed as part of Al Qa'ida (AQ). However on 2 February 2014, AQ senior leadership issued a statement officially severing ties with ISIL. This prompted consideration of the case to proscribe ISIL in its own right.

ISIL not only poses a threat from within Syria but has made significant advances in Iraq. The threat from ISIL in Iraq and Syria is very serious and shows clearly the importance of taking a strong stand against the extremists.

We are aware that a number of British nationals have travelled to Syria and some of these will inevitably be fighting with ISIL. It appears that ISIL is treating Iraq and Syria as one theatre of conflict and its potential ability to operate across the border must be a cause of concern for the whole international community.

In April 2014, ISIL claimed responsibility for a series of blasts targeting a Shia election rally in Baghdad. These attacks are reported to have killed at least 31 people. Thousands of Iraqi civilians lost their lives to sectarian violence in 2013, and attacks carried out by ISIL will have accounted for a large proportion of these deaths.

ISIL has reportedly detained dozens of foreign journalists and aid workers. In September 2013, members of the group kidnapped and killed the commander of Ahrar ash-Sham after he intervened to protect members of a Malaysian Islamic charity.

In January 2014, ISIL captured the Al-Anbar cities of Ramadi and Fallujah, and is engaged in ongoing fighting with the Iraqi security forces. The group also claimed responsibility for a car bomb attack that killed four people and wounded dozens in the southern Beirut suburb of Haret Hreik.

ISIL has a strong presence in northern and eastern Syria where it has instituted strict Sharia law in the towns under its control. The group is responsible for numerous attacks and a vast number of deaths. The group is believed to attract foreign fighters, including Westerners, to the region. The group has maintained control of various towns on the Syrian/Turkish border allowing the group to control who crosses and ISIL's presence there has interfered with the free flow of humanitarian aid.

Note: The Government laid an Order in August 2014 which provides that "Islamic State (Dawlat al Islamiya)" should be treated as another name for the organisation which is already proscribed as ISIL. The UK does not recognise ISIL's claims of a 'restored' Caliphate or a new Islamic State.

Jaish e Mohammed (JeM) and splinter group Khuddam Ul-Islam (Kul) – JeM proscribed March 2001 and Kul proscribed October 2005

JeM and Kul seek the ‘liberation’ of Kashmir from Indian control as well as the ‘destruction’ of America and India. JeM has a stated objective of unifying the various Kashmiri militant groups.

Jamaah Anshorut Daulah – Proscribed July 2016

JAD was established in March 2015 following the merger of several Indonesian extremist and terrorist groups aligned to Daesh. JAD has extensive links to Daesh and actively recruits fighters in Syria.

The group is led by the imprisoned extremist cleric Aman Abdurrahman and has close ties to other terrorist groups including Daesh. Its membership includes several former Jemaah Islamiyah (JI) members. JI were responsible for the 2002 and 2005 Bali attacks.

JAD was responsible for the attack near Sarinah Mall in Jakarta in January 2016, which was claimed by Daesh and resulted in the deaths of seven people (including the five attackers) and 20 people (including five police officers) being injured.

Jamaat ul-Ahrar (JuA) – Proscribed March 2015

JuA is a militant Islamist group that split away from Tehrik-e-Taliban Pakistan (TTP) in August 2014. JuA aims to establish an Islamic caliphate in Pakistan and aspires to extend global jihad into the Indian subcontinent.

The group have claimed responsibility for a number of recent attacks, including on 21 November 2014, a grenade attack on the Muttahida Qaumi Movement (MQM) in Orangi Town area of Karachi that killed three members of the Sindh Assembly and injured 50 workers; on 7 November 2014, twin bombings targeting peace committee volunteers in Chinari village of Safi Tehsil in the Mohmand Agency killed at least six people. JuA’s spokesman, Ehsanullah Ehsan, claimed responsibility and vowed to continue attacking tribal peace committees; and on 2 November 2014, the suicide bomber attack on the Pakistan side of Wagah border crossing, shortly after the famous flag-lowering ceremony had concluded, that killed over 60 people.

In September 2014, Ehsanullah Ehsan released a statement criticising the British Government for arresting Al Muhajiroun (ALM) associates and made a threat, stating that “your future security depends upon how nicely you treat the Muslims in Britain”.

In March 2015 the group claimed responsibility for fatal attacks on Christian sites in Lahore.

Jammat-ul Mujahideen Bangladesh (JMB) – Proscribed July 2007

JMB first came to prominence on 20 May 2002 when eight of its members were arrested in possession of petrol bombs. The group has claimed responsibility for numerous fatal bomb attacks across Bangladesh in recent years, including suicide bomb attacks in 2005.

Jamaat Ul-Furquan (JuF) – Proscribed October 2005

The aim of JuF is to unite Indian administered Kashmir with Pakistan; to establish a radical Islamist state in Pakistan; the ‘destruction’ of India and the USA; to recruit new jihadis; and the release of imprisoned Kashmiri militants.

Jaysh al Khalifatu Islamiya (JKI) which translates as the Army of the Islamic Caliphate –proscribed November 2014

JKI is an Islamist jihadist group, consisting predominately of Chechen fighters. JKI is an opposition group active in Syria.

JKI splintered from Jaysh al-Muhajireen Wal Ansar (JAMWA) in 2013. At that point a number of members went with Umar Shishani (aka Umar the Chechen) to join the Islamic State of Iraq and the Levant (ISIL) and, the rest of the group stayed distinct and renamed itself Majahideen of the Caucasus and the Levant (MCL) and more recently renamed itself JKI.

Before his death in 2014, JKI was led by Seyfullah Shishani, who had pledged allegiance to the leader of the Al Nusra Front, Mohammed Al-Jawlani. JKI has assisted ANF and ISIL in conducting attacks.

In February 2014, a British individual linked to the group, carried out a suicide attack on a prison in Aleppo, resulting in prisoner escapes.

Jeemah Islamiyah (JI) – Proscribed November 2002

JI’s aim is the creation of a unified Islamic state in Singapore, Malaysia, Indonesia and the Southern Philippines.

Jund al-Aqsa (JAA) which translates as “Soldiers of al-Aqsa” – Proscribed January 2015

JAA is a splinter group of Al Nusra Front (ANF), active in Syria against the Syrian Government since September 2013. JAA is a foreign fighter battalion of a variety of nationalities, as well as a native Syrian contingent. The group is primarily operating in Idlib and Hama.

JAA is believed to be responsible for the attack on 9 February 2014 in Maan village killing 40 people of which 21 were civilians. JAA and Ahrar al-Sham are reported to have uploaded YouTube footage of their joint offensive against the village, although neither group has claimed responsibility.

JAA has supported the Islamic Front in an operation to seize Hama military airport during July 2014. ANF released a document summarising its operations in August 2014, which included details of an attack that targeted a resort hotel conducted in collaboration with JAA.

Jund al Khalifa-Algeria (JaK-A) which translates as Soldiers of the Caliphate –
Proscribed January 2015

JaK-A is an Islamist militant group believed to be made up of members of dormant Al Qa'ida (AQ) cells. JaK-A announced its allegiance to the Islamic State of Iraq and Levant (ISIL) in a communiqué released on 13 September 2014.

In April 2014, JaK-A claimed responsibility for an ambush on a convoy, that killed 11 members of the Algerian army. On 24 September 2014, the group beheaded a mountaineering guide, Hervé Gourdel, a French national. The abduction was announced on the same day that a spokesman for ISIL, warned that it would target Americans and other Western citizens, especially the French, after French jets joined the US in carrying out strikes in Iraq on ISIL targets.

Kateeba al-Kawthar (KaK) also known as 'Ajnad al-sham' and 'Junud ar-Rahman al Muhajireen'- *Proscribed June 2014*

KaK describes itself as a group of mujahideen from more than 20 countries seeking a 'just' Islamic nation.

KaK is an armed terrorist group fighting to establish an Islamic state in Syria. The group is aligned to the most extreme groups operating in Syria and has links to Al Qa'ida.

The group's leader is described as a Western Mujaadid commander. KaK is believed to attract a number of Western foreign fighters and has released YouTube footage encouraging travel to Syria and asking Muslims to support the fighters.

Partiya Karkeren Kurdistanî (PKK) which translates as the Kurdistan Worker's Party –
Proscribed March 2001

PKK/KADEK/KG is primarily a separatist movement that seeks an independent Kurdish state in southeast Turkey. The PKK changed its name to KADEK and then to Kongra Gele Kurdistan, although the PKK acronym is still used by parts of the movement.

Note: The Government laid an Order in 2006 which provides that KADEK and Kongra Gele Kurdistan should be treated as another name for the organisation which is already proscribed as PKK.

Lashkar e Tayyaba (LT) – *Proscribed March 2001*

LT seeks independence for Kashmir and the creation of an Islamic state using violent means.

Note: The Government laid an Order in March 2009 which provides that Jama'at' ud Da'wa (JuD) should be treated as another name for the organisation which is already proscribed as Lashkar e Tayyaba.

Liberation Tigers of Tamil Eelam (LTTE) – Proscribed March 2001

The LTTE is a terrorist group fighting for a separate Tamil state in the North and East of Sri Lanka.

Libyan Islamic Fighting Group (LIFG) – Proscribed October 2005

The LIFG seeks to replace the current Libyan regime with a hard-line Islamic state. The group is also part of the wider global Islamist extremist movement, as inspired by Al Qa'ida. The group has mounted several operations inside Libya, including a 1996 attempt to assassinate Mu'ammarr Qadhafi.

Minbar Ansar Deen (also known as Ansar al-Sharia UK) – Proscribed July 2013

Minbar Ansar Deen is a Salafist group based in the UK that promotes and encourages terrorism. Minbar Ansar Deen distributes content through its online forum which promotes terrorism by encouraging individuals to travel overseas to engage in extremist activity, specifically fighting. The group is not related to Ansar al-Sharia groups in other countries.

Mujahidin Indonesia Timur (MIT) which translates as Mujahideen of Eastern Indonesia – Proscribed July 2016

MIT is Indonesia's most active terrorist group based in the mountainous jungle of Poso, in Central Sulawesi. Its leader, Abu Warda also known as Santoso, is one of Indonesia's most wanted terrorist. The group's modus operandi is to attack the police and the army which includes the use of explosives (including the use of IEDs), and shootings. MIT have been responsible for deaths of more than a dozen police officers in Poso in the last three years. They have also used kidnappings and beheadings of Christian farmers in Poso to dissuade the local populace from assisting the police.

MIT pledged its allegiance to Daesh in July 2014 and are assessed to have links to other Daesh affiliated terrorist groups in the region. MIT has claimed responsibility for a number of recent attacks and has threatened attacks on targets across the country including the capital (specifically the Jakarta police headquarters and the presidential palace in a video uploaded on 22 November 2015).

In September 2015 MIT was banned as a terrorist group by the USA and the UN.

National Action – Proscribed December 2016

National Action is a racist neo-Nazi group that was established in 2013. It has a number of branches across the UK, which conduct provocative street demonstrations and stunts aimed at intimidating local communities. Its activities and propaganda materials are particularly aimed at recruiting young people.

The group is virulently racist, anti-Semitic and homophobic. Its ideology promotes the idea that Britain will inevitably see a violent 'race war', which the group claims it will be an active

part of. The group rejects democracy, is hostile to the British state and seeks to divide society by implicitly endorsing violence against ethnic minorities and perceived ‘race traitors’.

National Action’s online propaganda material, disseminated via social media, frequently features extremely violent imagery and language. It condones and glorifies those who have used extreme violence for political or ideological ends. This includes tweets posted by the group in 2016, in connection with the murder of Jo Cox (which the prosecutor described as a terrorist act), stating “Only 649 MPs to go” and a photo of Thomas Mair with the caption “don’t let this man’s sacrifice go in vain” and “Jo Cox would have filled Yorkshire with more subhumans!”, as well as an image condoning and celebrating the terrorist attack on the Pulse nightclub in Orlando and another depicting a police officer’s throat being slit. The images can reasonably be taken as inferring that these acts should be emulated and therefore amount to the unlawful glorification of terrorism.

Palestinian Islamic Jihad – Shaqaqi (PIJ) – Proscribed March 2001

PIJ aims to end the Israeli occupation of Palestine and to create an Islamic state. It opposes the existence of the state of Israel, the Middle East Peace Process and the Palestinian Authority, and has carried out suicide bombings against Israeli targets.

Popular Front for the Liberation of Palestine-General Command (PFLP-GC) – Proscribed June 2014

PFLP-GC is a left wing nationalist Palestinian militant organisation formed in 1968. It is based in Syria and was involved in the Palestine intifada during the 1970s and 1980s. The group is separate from the similarly named Popular Front for the Liberation of Palestine (PFLP).

From its outset, the group has been a Syrian proxy. PFLP-GC has been fighting in the Syrian war in support of Assad, including in Yarmouk Refugee Camp in July 2013. The group also issued statements in support of the Syrian government, Hizballah, and Iran.

Revolutionary Peoples’ Liberation Party – Front (Devrimci Halk Kurtulus Partisi – Cephesi) (DHKP-C) – Proscribed March 2001

DHKP-C aims to establish a Marxist-Leninist regime in Turkey by means of armed revolutionary struggle.

Salafist Group for Call and Combat (Groupe Salafiste pour la Predication et le Combat) (GSPC) – Proscribed March 2001

Its aim is to create an Islamic state in Algeria using all necessary means, including violence.

Saved Sect or Saviour Sect – Proscribed July 2006

The Saved Sect /Al Ghurabaa is an Islamist group which seeks to establish an Islamic Caliphate ruled by Shariah law. The group first emerged as Al Muhajiroun in the UK, in 1996, led by Omar Bakri Muhammed, who then publicly disbanded the organisation in 2004. The

organisation reformed in 2004 under the names Al Ghurabaa and the Saved Sect. While the Group has some links to groups overseas, it is based and operates within the UK.

Note: The Government laid Orders, in January 2010 and November 2011, which provide that **Al Muhajiroun, Islam4UK, Call to Submission, Islamic Path, London School of Sharia** and **Muslims Against Crusades** should be treated as alternative names for the organisation which is already proscribed under the names Al Ghurabaa and **The Saved Sect**.

Sipah-e Sahaba Pakistan (SSP) (Aka Millat-e Islami Pakistan (MIP) – SSP was renamed MIP in April 2003 but is still referred to as SSP) and splinter group Lashkar-e Jhangvi (LeJ) – Proscribed March 2001

The aim of both SSP and LeJ is to transform Pakistan by violent means into a Sunni state under the total control of Sharia law. Another objective is to have all Shia declared Kafirs and to participate in the destruction of other religions, notably Judaism, Christianity and Hinduism.

Kafirs means non-believers: literally, one who refused to see the truth. LeJ does not consider members of the Shia sect to be Muslim, so concludes they can be considered a 'legitimate' target.

Note: The Government laid an Order in October 2013 which provides that Ahle Sunnat wal Jamaat (ASWJ) should be treated as another name for the organisation which is already proscribed as Sipah-e Sahaba Pakistan (SSP) and Lashkar-e Jhangvi (LeJ).

Tehrik Nefaz-e Shari'at Muhammadi (TNSM) – Proscribed July 2007

TNSM regularly attacks coalition and Afghan government forces in Afghanistan and provides direct support to Al Qa'ida and the Taliban. One faction of the group claimed responsibility for a suicide attack on an army training compound on 8 November 2007 in Dargai, Pakistan, in which 42 soldiers were killed.

Tehrik-e Taliban Pakistan (TTP) – Proscribed January 2011

Tehrik-e Taliban Pakistan has carried out a high number of mass casualty attacks in Pakistan and Afghanistan since 2007. The group have announced various objectives and demands, such as the enforcement of sharia, resistance against the Pakistani army and the removal of NATO forces from Afghanistan. The organisation has also been involved in attacks in the West, such as the attempted Times Square car-bomb attack in May 2010.

Teyre Azadiye Kurdistan (TAK) – Proscribed July 2006

TAK is a Kurdish terrorist group currently operating in Turkey.

Turkestan Islamic Party (TIP) also known as East Turkestan Islamic Party (ETIP), East Turkestan Islamic Movement (ETIM) and Hizb al-Islami al-Turkistani (HAAT) – Proscribed July 2016

TIP is an Islamic terrorist and separatist organisation founded in 1989 by Uighur militants in western China. It aims to establish an independent caliphate in the Uighur state of Xinjiang Uighur Autonomous Region of North-western China and to name it East Turkestan. TIP is based in the Federally Administered Tribal Areas (FATA) of Pakistan, and operates in China, Central and South Asia and Syria. The group has claimed responsibility for a number of attacks in China, the latest of these being in April 2014. TIP has links to a number of terrorist groups including Al Qa'ida (AQ).

In November 2015, TIP released the 18th issue of its magazine 'Islamic Turkestan' through the Global Islamic Media Front (GIMF), detailing TIP's jihad against the Chinese authorities. Video footage from September 2015 shows TIP hosting training camps in areas controlled by the Pakistani Taliban in North Waziristan.

More recently TIP has maintained an active and visible presence in the Syrian war and has published a number of video clips of its activities. Examples of this from March to April 2016 include:

- TIP claiming a joint attack with Jund al Aqsa in Sahl al Ghab and published a video of a suicide bomb attack in April 2016;
- a video published in March 2016 which promotes the victories of TIP in Syria and calls for Muslims to join jihad; and
- a video slide show published in April 2016 which shows fighters and children in training.

TIP has been banned by the UN and is also sanctioned by the USA under the Terrorist Exclusion list.

Turkiye Halk Kurtulus Partisi-Cephesi (THKP-C) is also known as the Peoples' Liberation Party/Front of Turkey, THKP-C Acilciler and the Hasty Ones – Proscribed June 2014

THKP-C is a left wing organisation formed in 1994. The group grew out of the Turkish extreme left Revolutionary Youth Movements which formed in the 1960s and 70s.

THKP-C now also operates as a pro-Assad militia group fighting in Syria and has developed increased capability since the Syrian insurgency. THKP-C is assessed to have been involved in an attack in Reyhanli, Turkey, in May 2013, killing over 50 people and injuring over 100.

The organisation has always been most prominent in the southern province of Hatay. A number of other groups have been formed under the THKP-C umbrella including 'Mukavament Suriye' (Syrian Resistance), which is reported to have been responsible for the recent Baniyas Massacre killing at least 145 people.

ORGANISATIONS LINKED TO NORTHERN IRELAND RELATED TERRORISM

Continuity Army Council
Cumann na mBan
Fianna na hEireann
Irish National Liberation Army
Irish People's Liberation Organisation
Irish Republican Army
Loyalist Volunteer Force
Orange Volunteers
Red Hand Commando
Red Hand Defenders
Saor Eire
Ulster Defence Association
Ulster Freedom Fighters
Ulster Volunteer Force

ANNEX C – Total Items of Communications Data under Chapter 2 of Part 1 of RIPA by Public Authority

This Annex details the total items of data acquired by each public authority in 2015, as set out in the Report of the Interception of Communications Commissioner for 2015.

Public authorities have only been required to provide statistical details about the number of items of data since 25 March 2015 when the revised Code of Practice came into force. Consequently, some public authorities were only able to give the total items of data approved from the 1 April 2015 (three quarters of the year), rather than from the 1 January (the full four quarters of the year).

Where this was the case, and in order to provide comparable figures, the three quarter totals were ‘projected’ in the Commissioner’s Report to make up the difference. This was achieved simply by multiplying the three quarter totals by 1.333r. Any statistics which were projected are shown in red and the three quarter figure reported by the public authority is displayed in the adjacent column.

Police Forces and Law Enforcement Agencies

| | Total items of data [projected] | Partial figure reported 01/04/15– 31/12/15 | | Total items of data [projected] | Partial figure reported 01/04/15– 31/12/15 |
|------------------------------|------------------------------------|--------------------------------------------------|-----------------------------------------|------------------------------------|--------------------------------------------------|
| Avon & Somerset Constabulary | 15,277 | 11,458 | Metropolitan Police | 107,362 | – |
| Bedfordshire Police | 3,791 | 2,843 | Ministry of Defence Police | 136 | – |
| British Transport Police | 2,900 | 2,175 | National Crime Agency (NCA) | 64,116 | 48,087 |
| Cambridgeshire Constabulary | 4,109 | 3,082 | Norfolk Constabulary & Suffolk Police** | 6,499 | 4,874 |
| Cheshire Constabulary* | 10,604 | 7,953 | North Wales Police | 6,928 | – |
| City of London Police | 4,065 | 3,049 | North Yorkshire Police | 5,269 | 3,952 |
| Cleveland Police | 10,852 | 8,139 | Northamptonshire Police | 7,063 | – |
| Cumbria Constabulary | 3,876 | – | Northumbria Police | 9,853 | – |
| Derbyshire Constabulary | 6,459 | – | Nottinghamshire Police | 16,762 | – |
| Devon & Cornwall Police | 20,895 | 15,671 | Police Scotland | 51,719 | – |
| Dorset Police | 3,739 | 2,804 | Police Service of Northern Ireland | 8,813 | 6,610 |

| | Total items of data [projected] | Partial figure reported 01/04/15– 31/12/15 | | Total items of data [projected] | Partial figure reported 01/04/15– 31/12/15 |
|----------------------------------------|--------------------------------------------|-----------------------------------------------------------|--------------------------------------------|--------------------------------------------|-----------------------------------------------------------|
| Durham Constabulary | 7,676 | – | Royal Air Force Police | 9 | 7 |
| Dyfed Powys Police | 3,104 | 2,328 | Royal Military Police | 356 | – |
| Gloucestershire Constabulary | 2,756 | 2,067 | Royal Navy Police | 45 | 34 |
| Greater Manchester Police | 33,143 | 24,857 | South Wales Police | 17,368 | 13,026 |
| Gwent Police | 5,315 | 3,986 | South Yorkshire Police | 8,225 | 6,169 |
| Hampshire Constabulary | 12,813 | – | Staffordshire Police | 9,350 | – |
| Hertfordshire Constabulary | 14,581 | – | Surrey Police | 8,896 | 6,672 |
| Her Majesty's Revenue & Customs (HMRC) | 12,191 | – | Sussex Police | 5,305 | 3,979 |
| Humberside Police | 5,436 | 4,077 | Thames Valley Police | 11,983 | 8,987 |
| Kent Police & Essex Police** | 20,067 | – | Home Office (Immigration Enforcement) | 6,113 | 4,585 |
| Lancashire Constabulary | 19,672 | 14,754 | Warwickshire Police & West Mercia Police** | 18,996 | – |
| Leicestershire Police | 8,637 | 6,478 | West Midlands Police | 45,238 | – |
| Lincolnshire Police | 4,444 | 3,333 | West Yorkshire Police | 31,673 | 23,755 |
| Merseyside Police | 24,780 | 18,585 | Wiltshire Police | 4,472 | 3,354 |
| Grand Total | | | | 713,731 | |

*Cheshire Constabulary's total items do not include items approved orally, so will be higher than the figures presented.

**Some police forces share the services of a SPoC, and where this is so combined figures are reported.

Having lost their powers on 12 February 2015, the Civil Nuclear Constabulary, the Port of Dover Police and the Port of Liverpool Police all reported that they did not approve any items of data between 1 January and 12 February 2015.

Intelligence Agencies

| | Total items of data (projected) | Partial figure reported 01/04/15- 31/12/15 |
|---------------------------------------|--------------------------------------------|-----------------------------------------------------------|
| GCHQ | 4,268 | 3,201 |
| The Secret Intelligence Service (MI6) | 531 | – |
| The Security Service (MI5) | 38,317 | – |
| Grand Total | 43,116 | |

Other Public Authorities

| | Total items of data (projected) | Partial figure reported 01/04/15- 31/12/15 | | Total items of data (projected) | Partial figure reported 01/04/15- 31/12/15 |
|-----------------------------------------------------------------|--------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------|--------------------------------------------|-----------------------------------------------------------|
| Air Accident Investigation Branch | 21 | – | Information Commissioner's Office | 24 | – |
| Competition and Markets Authority | 87 | – | Maritime & Coastguard Agency | 6 | – |
| Criminal Cases Review Commission | 11 | – | Medicines and Healthcare Products Regulatory Agency | 228 | 171 |
| Department of Enterprise, Trade & Investment (Northern Ireland) | 101 | 76 | Ministry of Justice – National Offender Management Service | 75 | – |
| Department of Work & Pensions Child Maintenance Group | 14 | – | NHS Protect | 16 | – |
| Financial Conduct Authority | 2,808 | – | Office of Communications | 27 | – |
| Gambling Commission | 36 | – | Office of the Ombudsman for Northern Ireland | 18 | – |
| Gangmasters Licensing Authority | 82 | – | Rail Accident Investigation Branch | 11 | – |

| | Total items of data (projected) | Partial figure reported 01/04/15- 31/12/15 | | Total items of data (projected) | Partial figure reported 01/04/15- 31/12/15 |
|------------------------------------------|------------------------------------|--------------------------------------------------|----------------------|------------------------------------|--------------------------------------------------|
| Health & Safety Executive | 7 | – | Royal Mail* | 28 | – |
| Independent Police Complaints Commission | 30 | – | Serious Fraud Office | 250 | – |
| Grand Total | | | | 3,880 | |

*Royal Mail lost its powers to acquire communications data on 12/02/2015 and the figure reported here represents items acquired between 01 January and 12 February 2015.

As outlined in the Commissioner's Report, the following "other" public authorities reported that they did not acquire any communications data during 2015 (those in orange also lost their powers on 12/02/2015):

- Charity Commission
- Department for the Environment, Food & Rural Affairs
- Department for Business, Innovation & Skills
- Department of the Environment (Northern Ireland)
- Department of Agriculture & Rural Development (Northern Ireland)
- Environment Agency
- Food Standards Agency
- Marine Accident Investigation Branch
- NHS Scotland
- Northern Ireland Health & Social Services Central Services Agency
- Northern Ireland Office – Northern Ireland Prison Service
- Police Investigations Review Commissioner
- Prudential Regulation Authority
- Scottish Criminal Cases Review Commissioner
- Scottish Environmental Protection Agency
- The Pensions Regulator
- No Fire Authority
- No Ambulance Service or Trust

Local Authorities

| | | | |
|----------------------------------------|-----|-------------------------------------------|------------|
| Aberdeenshire Council | 2 | London Borough of Camden Council | 1 |
| Barnsley Metropolitan Council | 9 | London Borough of Croydon Council | 31 |
| Bedford Borough Council | 4 | London Borough of Enfield Council | 3 |
| Birmingham City Council | 52 | London Borough of Harrow Council | 3 |
| Bracknell Forest Borough Council | 1 | London Borough of Redbridge | 8 |
| Bristol City Council | 2 | Merthyr Tydfil County Borough Council | 3 |
| Bromsgrove District Council | 30 | Milton Keynes Borough Council | 3 |
| Buckinghamshire County Council | 7 | North Kesteven District Council | 8 |
| Bury Metropolitan Borough Council | 2 | North Lincolnshire Council | 6 |
| Caerphilly County Borough Council | 3 | North Yorkshire County Council | 4 |
| Cambridgeshire County Council | 4 | Northamptonshire County Council | 6 |
| Cardiff City and County Council | 15 | Northumberland County Council | 14 |
| Ceredigion County Council | 2 | Nottinghamshire County Council | 15 |
| Cheshire East Council | 4 | Oldham Metropolitan Borough Council | 4 |
| Cheshire West & Chester Council | 9 | Oxfordshire County Council | 31 |
| City of London Corporation | 13 | Poole Borough Council | 7 |
| Cornwall County Council | 15 | Portsmouth City Council | 8 |
| Darlington Borough Council | 6 | Redcar & Cleveland Borough Council | 30 |
| Devon County Council | 19 | Rhondda Cynon Taff County Borough Council | 41 |
| Dudley Metropolitan Borough Council | 10 | Rotherham Borough Council | 1 |
| Durham County Council | 37 | Shropshire Council | 6 |
| East Riding of Yorkshire Council | 9 | South Gloucestershire Council | 1 |
| Flintshire County Council | 1 | Staffordshire County Council | 61 |
| Gateshead Metropolitan Borough Council | 15 | Stockport Metropolitan Borough Council | 2 |
| Glasgow City Council | 2 | Stockton-on-Tees Borough Council | 5 |
| Gloucestershire County Council | 12 | Stoke-on-Trent City Council | 13 |
| Hampshire County Council | 3 | Suffolk County Council | 21 |
| Hertfordshire County Council | 5 | Swindon Borough Council | 5 |
| Hertsmere Borough Council | 2 | Thurrock Borough Council | 18 |
| Huntingdonshire District Council | 5 | Torfaen County Borough Council | 3 |
| Kent County Council | 107 | West Berkshire Council | 14 |
| Lancashire County Council | 15 | Wrexham County Borough Council | 6 |
| Leicestershire County Council | 71 | Warrington Council | 16 |
| Lincolnshire County Council | 6 | Warwickshire County Council | 3 |
| London Borough of Brent Council | 2 | Wealden District Council | 4 |
| London Borough of Bromley Council | 55 | York City Council | 14 |
| Grand Total | | | 975 |

ANNEX D – Decisions made in cases at the Investigatory Powers Tribunal, 2011-2015

| Year | New Cases Received | Cases Decided | Decision Breakdown |
|------|--------------------|---------------|-----------------------------------------------------------------|
| 2011 | 180 | 196 | 86 (44%) were ruled as 'frivolous or vexatious' |
| | | | 72 (36%) received a 'no determination' outcome |
| | | | 20 (10%) were ruled out of jurisdiction |
| | | | 11 (6%) were ruled out of time |
| | | | 3 (2%) were withdrawn |
| | | | 2 (1%) were judged to be not a valid complaint |
| | | | 2 (1%) were found in favour |
| 2012 | 168 | 191 | 100 (52.5%) were ruled as 'frivolous or vexatious' |
| | | | 62 (32.5%) received a 'no determination' outcome |
| | | | 14 (7%) were ruled out of jurisdiction |
| | | | 9 (5%) were ruled out of time |
| | | | 5 (2.5%) were withdrawn |
| | | | 1 (0.5%) were judged to be not a valid complaint |
| 2013 | 205 | 161 | 85 (53%) were ruled as frivolous or vexatious |
| | | | 50 (31%) received a 'no determination' outcome |
| | | | 17 (10%) were ruled out of jurisdiction, withdrawn or not valid |
| | | | 9 (6%) were ruled out of time |
| 2014 | 215 | 201 | 104 (52%) were ruled as frivolous or vexatious |
| | | | 53 (26%) received a 'no determination' outcome |
| | | | 36 (18%) were ruled out of jurisdiction, withdrawn or not valid |
| | | | 8 (4%) were ruled out of time |
| 2015 | 251 | 219 | 101 (47%) were ruled as frivolous or vexatious |
| | | | 65 (30%) received a 'no determination' outcome |
| | | | 38 (17%) were ruled out of jurisdiction, withdrawn or not valid |
| | | | 7 (3%) were ruled out of time |
| | | | 8 (4%) were found in favour |

Please note: Any differences between the statistics published here and those of the previous report are the result of corrections that have since been made on the Investigatory Powers Tribunal website www.ipt-uk.com.



HM Government

ISBN 978-1-4741-4093-5



9 781474 140935