



THE GOVERNMENT REPLY TO THE SIXTH  
REPORT FROM THE HOME AFFAIRS COMMITTEE  
SESSION 2009-10 HC 117

# **The Home Office's Response to Terrorist Attacks**

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

**February 2010**



THE GOVERNMENT REPLY TO THE SIXTH  
REPORT FROM THE HOME AFFAIRS COMMITTEE  
SESSION 2009-10 HC 117

# **The Home Office's Response to Terrorist Attacks**

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

**February 2010**

**© Crown Copyright 2010**

The text in this document (excluding the Royal Arms and other departmental or agency logos) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

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

For any other use of this material please contact the Office of Public Sector Information, Information Policy Team, Kew, Richmond, Surrey TW9 4DU  
or e-mail: [licensing@opsi.gsi.gov.uk](mailto:licensing@opsi.gsi.gov.uk).

ISBN: 9780101778824

Printed in the UK by The Stationery Office Limited  
on behalf of the Controller of Her Majesty's Stationery Office

ID P002348987 02/10 1685 19585

Printed on paper containing 75% recycled fibre content minimum.

# **GOVERNMENT REPLY TO THE SIXTH REPORT FROM THE HOME AFFAIRS COMMITTEE SESSION 2009-10 HC 117**

## **THE HOME OFFICE'S RESPONSE TO TERRORIST ATTACKS**

### **INTRODUCTION**

The House of Commons Home Affairs Committee (HAC) published the report of its inquiry into the Home Office's Response to Terrorist Attacks on 2 February 2010.

The inquiry considered aspects of the Government's counter-terrorism work, focussing in particular on the following issues:

- The immediate response of the Home Office to a terrorist attack, including the effectiveness of the Civil Contingencies Committee (COBR) co-ordinating an immediate Government response;
- The potential use of intercept as evidence and the value of control orders;
- The misuse and misapplication of anti-terrorism powers; and
- Anti-terrorism measures at the European level.

This Command Paper sets out the Government response to the conclusions and recommendations in the Committee's report.

The first priority of any Government is to ensure the security and safety of the nation and all members of the public. The Government welcomes the contribution of the HAC to this important work but rejects some of the claims made in its report. These are addressed below.

The Government is aware of the threat this country faces from international terrorism and has effective systems and processes in place to deal with it. On 24 March 2009 the Government published a revised and updated version of CONTEST, its strategy for countering international terrorism. CONTEST sets out the principles that govern our response to the threat of terrorism, emphasising our commitment to human rights and the rule of law. The strategy outlines future programmes to address both the immediate threats from terrorism and its causes. CONTEST is one of the most comprehensive and wide-ranging approaches to tackling terrorism in the world. Just six months ago the Committee found it "first-class, effective and as "joined-up" as any system of government can expect."

The Government's strategy has had a practical and tangible impact:

### ***Pursue***

Since 2001, over 200 people (217) have been convicted of terrorist-related offences. The Police and the security and intelligence agencies have disrupted over a dozen attempted terrorist plots in the UK.

Considerable effort and resources have been devoted to building CT capacity: in recent years the number of Police dedicated to counter-terrorism work has grown by over 70% and the Security Service has doubled in size.

### ***Prevent***

To ensure we tackle not only the symptoms of terrorism but also its causes, we have significantly increased the scale of resources devoted to stopping people becoming terrorists or supporting violent extremism. In August 2009 we published revised guidance for local practitioners on how to deliver the *Prevent* strategy.

Our community-based response to violent extremism now extends across the country, reaching over 40,000 individuals; eight de-radicalisation projects are being piloted in nine areas; over 1000 community projects have received Local Authority funding.

The multi-agency Channel Project to support people assessed to be vulnerable to violent extremism now operates across 12 Police forces and over 75 Local Authorities, supporting just over two hundred people. Further guidance on Channel will be published shortly.

We have developed new ways of sharing information on radicalisation more widely than has previously been the case, using Counter-Terrorism Local Profiles made available for Local Government.

Communications are a vital part of our work on counter-terrorism. We have developed and launched a counter-narrative campaign with funding and support for organisations able to challenge the ideology of Al Qa'ida and other terrorist organisations.

### ***Protect and CBRNE***

We have quickly responded to the attempted attack on an airline on 25 December. Work is underway on watchlisting, explosives research, scanning technology and data sharing. The Government is engaged with counterparts in Europe and with the US and with industrial partners here. Work continues to develop responses to a terrorist attack of the kind that took place in Mumbai in November 2008.

The Government has allocated additional resources to develop a cadre of 250 Police Counter-Terrorism Security Advisors who have provided protective security advice to over 500 sports stadia, 600 shopping centres and 10,000 pubs and clubs. We launched a public consultation to look at how we could further protect our crowded places last year and will shortly be publishing our definitive guidance.

Contemporary terrorist organisations aspire to use chemical, biological, radiological and even nuclear weapons (CBRN). We have created "The Model Response to CBRN Events", a classified document which sets out an ideal response to a CBR attack to guide responding agencies and the emergency services. The thinking and rationale behind the "Model Response" is widely regarded as being world-leading amongst our international allies. We

have increased the numbers of CBRN-trained Police officers to over 8,000; CBRN training has been provided for 90% of Fire and Rescue personnel.

We have also created a national CBRN response centre, run by the Police. The centre has delivered into service over 280,000 items of CBRN equipment. Over 50 exercises have been managed or supported by the centre's exercise team. The centre runs a 24/7 operations and advice facility which has provided advice and support to over 80 incidents where suspected CBRN materials have been found. We are currently finalising a new strategy for countering the threat posed by CBRN weapons.

In August 2009, the Government released its Science and Technology Strategy for Countering International Terrorism, which sets out a number of horizon-scanning activities looking at emerging technologies to ensure our response to the threat remains relevant and flexible. We have launched INSTINCT (Innovative Science & Technology in Counter-Terrorism), a cross-Government programme which seeks innovative solutions from industry to support our CT strategy. That programme is widely regarded as having led to a step change in private sector engagement.

### ***Prepare***

To ensure we are fully prepared for a terrorist incident we continue to roll out a comprehensive counter-terrorism exercises programme. In 2009 we delivered three national-level CT exercises, along with a suite of preparatory training events and in 2010 we will deliver a further three major exercises. The scale of these exercises can be considerable – a major exercise can take between 9-12 months to organise, and involve 200-1000 participants.

### ***Olympics***

We have published an overarching Olympic Safety and Security Strategy that sets out our entire approach to what many believe is the single biggest security challenge that the UK has faced since the end of World War II. The Concept of Operations for Games Security (CONOPS) sets out a single vision for the delivery of Games time security at every venue, ensuring that there is a consistently high standard at both brand new and existing venues. The Strategy is being delivered on target and on budget. Successful security operations are already underway at the Olympic Park, protecting it now and preparing for a successful operation in 2012.

The Government recognises the importance of building on these successes in the future. We will continue to rapidly develop our work across all strands of the CONTEST strategy, adapting our response to the evolving threat. The protection of the British public is and will remain the Government's highest priority.

# GOVERNMENT'S RESPONSE TO THE COMMITTEE'S RECOMMENDATIONS

The Committee reached a number of conclusions and highlighted recommendations for action by the Government. In this response the recommendations are identified according to the paragraphs in which they appear in the conclusion of the report. Some responses are grouped together where they relate to the same issue.

## COBR

**1. While it is difficult to hold regular meetings during an emergency situation, we are surprised that two former senior policemen raised concerns over the frequency of COBRA meetings and suggested that the timing of meetings was unpredictable. We recommend that as far as possible a fixed schedule of regular meetings be maintained. Participants in COBRA meetings need to feed back the results of the main meeting and implement emergency plans—there is a danger, without a relatively fixed schedule, that COBRA gets in the way of this and actively hinders the operational response. (Paragraph 7)**

The Cabinet Office Briefing Room (COBR) is a well tried and tested mechanism for co-ordinating inter Departmental and inter agency responses to terrorist (and other) incidents in the UK and overseas. It provides for informed, collective decision-making (in real time) based on an agreed intelligence assessment and good situational awareness. It does not seek to duplicate the role of the blue light services which remain the cornerstone of any response to an emergency. The Government welcomes the Committee's conclusion that COBR is a good system.

One of the strengths of COBR is its ability to respond rapidly and appropriately to a wide range of different incidents. Arrangements are in place to ensure that COBR can meet at 1 hour's notice. It can be called in the anticipation of and not only after an event and can meet in a variety of formats and at different levels.

Following an incident the Cabinet Office liaises closely with the relevant Police Commander about the frequency and timing of COBR meetings to ensure that there is no adverse impact on operations and that the Police and Emergency Services benefit from timely decisions taken by central Government. Altering these arrangements to a more fixed schedule would make for a less dynamic response to emerging threats and risks imposing unnecessarily rigid timetables on emergency responders.

**2. A degree of demarcation exists between 'operational' and 'political' actors within COBRA. Formalising this may produce better informed decision-making, but we cannot see how further demarcation and "sub-groups" would be avoided, negating any advantages. As long as everyone involved in a COBRA meeting is aware of their roles (and we have no evidence that they are not) then we do not see any major problems caused by the current informal demarcation between "political" and "operational" actors. (Paragraph 9).**

We welcome the Committee's endorsement of the existing structures, which have been developed on the basis of lessons we have learned. As the Committee notes, additional structures would serve no useful purpose.

**3. It is imperative that key actors, especially Ministers who will be taking major decisions, experience a full "COBRA simulation" before facing a real-life incident. We are disappointed that the perception exists among some operational actors that the Home Secretary and other relevant Ministers have not participated as fully as could be expected in the exercise programme. We strongly recommend that in future, participation in such exercises becomes a key part of Ministerial life. (Paragraph 12)**

We welcome the Committee's endorsement of the importance of the exercise programme and the progress that has been made in this area of work in recent years. The Committee should be assured that participation in COBR exercises *is* recognised as an important Ministerial responsibility. The Home Secretary and other relevant Ministers (Bill Rammell MP, Minister of State for the Armed Forces, and Lord West, Parliamentary Under Secretary of State for Security and Counter-Terrorism) all participated in the most recent counter-terrorism exercise.

**4. As a forum for co-ordinating information after a terrorist attack, COBRA is as good a system as possible, and aside from the minor technical issues we have noted concerning the timing of meetings and participation in exercises we have no complaints with how it operates. (Paragraph 13)**

The Government again welcomes the Committee's endorsement of the COBR system. The COBR concept is rightly regarded as a model of how government should set the strategic direction and co-ordinate efforts to respond to a terrorist incident.

## **CO-ORDINATING AN IMMEDIATE RESPONSE TO ATTACKS**

**5. The Weekly Security Meeting—a meeting of which we were previously unaware—performs many of the functions that a National Security Committee would perform; in effect a de facto National Security Committee already exists and functions, however discreetly. (Paragraph 14)**

**6. While we are not placed to comment on the effectiveness of the Weekly Security Meeting, the lack of public awareness of its existence is troubling. The public have a right to know who is protecting them from terrorist threats and in turn, those protecting the public should expect to be accountable and have their performance reviewed. To achieve these aims we propose the transformation of the "Weekly Security Meeting" into a more formalised, standing body known as the "National Security Committee", chaired by the Home Secretary or Prime Minister who would invite outside, non-governmental experts to attend as the situation arises. The work of this Committee should also be assisted by**

**prominent appointed National Security Advisers who could also be fully accountable to Parliament. (Paragraph 15)**

The inception of the Weekly Security Meeting, chaired by the Home Secretary, was announced to Parliament by the then Prime Minister on 29 March 2007. The former Home Secretary, Dr John Reid MP, also mentioned the Weekly Security Meeting in April 2007 during his evidence to the Home Affairs Committee and its role is described in our publicly available 2009 counter-terrorism strategy, CONTEST (page 138).

The Weekly Security Meeting is attended by senior representatives of the intelligence agencies, the Police and key Government departments involved in CT. The meeting provides an opportunity for Home Office Ministers and the wider Whitehall CT Community, to be updated on the latest threat to the UK (including highly classified intelligence reporting) and current policy responses. It is not a decision making body.

It may be helpful to set out how counter-terrorism governance and oversight operates in this country.

Day to day Ministerial oversight of CONTEST rests with the Home Secretary as the lead Minister for counter terrorism. Oversight is further provided through NSID, chaired by the Prime Minister, and including the Home and Foreign Secretaries, the Chancellor, other relevant Ministers, the heads of the security and intelligence agencies, the military and ACPO as appropriate. NSID is responsible for considering all aspects of counter-terrorism and national security policy.

NSID may also receive external advice on counter-terrorism and other national security issues, from the National Security Forum, an independent body of outside advisors with expertise on many aspects of national security.

NSID is supported by a series of committees of officials modelled on the structure of CONTEST. The CONTEST Board is chaired by the Director General of OSCT. These committees are concerned with the development and implementation of the strategy and for oversight of key programmes. Much of their work is sensitive and classified and for security and operational reasons cannot be made available to the public.

Planning and decision making for counter-terrorism *operations* (not overall strategy and programme management) is the responsibility of the Police and the security and intelligence agencies. The Police and the Agencies have in place mechanisms to ensure appropriate national coordination. Operational work, as detailed above, is briefed into the Weekly Security Meeting.

Distinct from strategic planning, programme management and operational planning, COBR coordinates crisis management for counter-terrorism and other emergencies.

In its analysis of the Government's counter terrorism structure, the Committee may have confused these different functions.

The Committee's own counter-terrorism sub-committee said in its report in July last year that: "based on the evidence we have taken both in public and in private, and the briefings we have received, we are satisfied that the UK's counter-terrorism apparatus is first-class, effective and as 'joined-up' as any system of government can expect. We have considerable confidence in OSCT and in its liaison with other departments and agencies."

We believe that the current structures provide clear responsibility for strategy, programme management, operations and crisis management, with very close Ministerial involvement at every level.

## **POLICING STRUCTURE**

**7. The Police must remember that while regional Counter-Terrorism Units (CTUs) may allow for an increase in the skills and expertise available to disrupt and prevent attacks happening, this expertise will be rendered useless without adequate information gathered from within communities. The creation of "supra-regional" bodies also carries the risk of breaking the vital link with local communities. Despite creating regional bodies, the Police must take every care to maintain the links with local communities which will be at the core of any intelligence gathering. (Paragraph 17)**

As AC John Yates said in his evidence to the Committee "the real power of the current network is that it is embedded at the local level" - with local forces working closely with their local communities on the one hand and the regional and national CT network providing higher level coordination on the other. Local forces contribute to the regional intelligence picture developed by Counter-Terrorism Units (CTUs) and Counter-Terrorism Intelligence Units (CTIUs) and have a vital role to play in supporting both the Security Service and the wider Police network's efforts to counter the terrorist threat.

We therefore welcome the Committee's endorsement of the valuable contribution that local forces and local communities make in the fight against terrorism. This is, and will continue to be, one of the strongest arguments for the current policing structures.

**8. We would like to know exactly when the development of regional counter-terrorism units was first considered by the Home Office and Police service. We remain unclear as to how much impetus the events of 2005 provided for this change. We must place on record our concern that the Government and the Police appear to have been lethargic in driving through necessary reforms to the policing system, and that there was insufficient political will to provide solutions. The Government and enforcement institutions must be proactive and identify problems themselves before a fatal attack acts as a catalyst for reform. (Paragraph 19)**

The Government has responded continuously to the evolving threat to the UK from international terrorism since the events of 9/11.

Significant changes were made prior to July 2005. Between September 2001 and July 2005 the Security Service increased in size by over 30% and began a programme of regionalisation. In policing, the post of National Coordinator Special Branch (NCSB) and Special Branch Regional Intelligence Cells (RICs) were all established in April 2003. These units were intended to improve regional coordination and were subsequently folded into the Counter-Terrorism Units (CTUs) and Counter-Terrorism Intelligence Units (CTIUs).

In 2004 Operations Crevice and Rhyme successfully disrupted two major AQ related terrorist plots that would otherwise have led to a significant loss of life in the UK. The unprecedented scale and complexity of these two operations prompted both the Security Service and the Police to make further structural changes.

In June 2004 work began on the West Midlands Counter-Terrorist Support Unit, an ACPO sponsored “pilot” of what was effectively a prototype CTU. This brought together intelligence and investigative functions whilst absorbing the West Midlands Regional Intelligence Cell and had responsibility for supporting both the West and East Midlands regions.

In February 2005 a project began that led to a merger in October 2006 of the Metropolitan Police Special Branch (SO12) and the Anti-Terrorist Branch (SO13) into SO15 or the Metropolitan Police Service Counter-Terrorism Command (CTC).

In April 2005 Greater Manchester Police set up its Anti-Terrorist unit to work alongside its Special Branch and the North West Regional Intelligence Cell in what was again effectively a prototype for the subsequent North West CTU.

It would therefore be incorrect to conclude that only the shocking and unprecedented events of 7/7 and 21/7 in 2005 led to organisational change in counter-terrorist work in the UK.

Building on work before 2005, a review by the Association of Chief Police Officers (ACPO) of the National Counter-Terrorism Structure in September 2006 proposed the establishment of three Counter-Terrorism Units (CTUs) in Manchester, Leeds and Birmingham to complement the MPS Counter-Terrorism Command in London. In response to operational demand a fourth CTU was added in the South East in 2009.

Alongside these structural changes, the number of Police personnel dedicated to counter-terrorism work has grown by over 70% in recent years, alongside the regional expansion of the Security Service.

No new security apparatus - least of all one dealing with counter-terrorism – can be developed successfully through anything other than an iterative process, based on learning and experience. It is wrong for the Committee to mistake this for ‘lethargy’ or conclude that it reflects ‘insufficient political will’.

**9. Many forces already rely on the Metropolitan Police for operational support. The primacy of the Metropolitan Police Service in counter-terrorism operations should be enshrined in statute. (Paragraph 24).**

The issue of the primacy of the Met in terrorist investigations has been considered on a number of occasions. It is the view of Government and the Police that any change in the law to create that primacy would not be 'relatively minor', as the Committee states, but would have major implications for UK policing – bearing on the role of Chief Constables, who are currently legally responsible and accountable for the direction of all policing activity in their own force area.

We have supported the professional view put forward by the Association of Chief Police Officers (ACPO) on the best way to organise the policing response to the international terrorist threat.

That view has been in favour of building an integrated national network of dedicated policing resources - where the Metropolitan Police Service has a pivotal role - which remains firmly connected to local policing and respects the authority of Chief Constables. This is the merit of the Police Counter-Terrorism Network, which combines regional Counter-Terrorism Units with co-ordination through the Metropolitan Police's National Coordinator for Terrorist Investigations.

Police across the country understand the clear and robust arrangements which are in place to react to and investigate any type of terrorist incident or investigation. The UK counter terrorism network continues to provide a full operational response to any incident. Chief Constables remain accountable for all operational matters within their own force area. In the event of a national multi-sited terrorist attack then the Assistant Commissioner Specialist Operations in the Metropolitan Police / Chair of ACPO (TAM) takes the operational lead, supported by colleagues both in Counter Terrorism Units and other forces across the country.

HMIC have concluded that the network of regional Police Counter-Terrorism Units and Counter-Terrorism Intelligence Units provides an appropriate base for conducting terrorist investigations.

**10. Successful counter-terrorism measures will rely on organisations working closely together and we are therefore pleased to hear that the many different bodies working on counter-terrorist activity are to a very great extent integrated. Whilst the creation of a National Terrorism Agency would remove the problem of co-ordinating the work of 52 separate Police forces, we see no great operational benefits through the formation of a single, national agency and the experience of the USA suggests that such an action is not a panacea. The problems which a National Terrorism Agency would claim to solve are, to our eyes, overstated, while the problems that it could cause are potentially very great. We remain convinced that Police skills and knowledge, rather than policing structures, are the key to preventing terrorism. (Paragraph 30)**

The Government agrees with this recommendation. The recent report from the Committee's own counter-terrorism sub-committee said that: "based on the evidence we have taken both in public and in private, and the briefings we have received, we are satisfied that the UK's counter-terrorism apparatus is

first-class, effective and as ‘joined-up’ as any system of government can expect.”

We believe that the current structures in place in this country give us the best of both worlds: OSCT acts as a co-ordinating hub, developing and tracking the progress of the overall strategy (CONTEST); individual departments and agencies carry out their own operations using their own considerable specialist expertise.

## USE OF INTERCEPT

Warranted interception of communications is a critical tool in protecting the public from terrorists and other serious criminals. It has been and remains the Government’s objective to build on the current successful use of interception by also enabling intercept material to be used as evidence in criminal trials. That is why in February 2008 the Government accepted the recommendations of the cross-party Privy Council Review, and set in train the necessary implementation process. At the same time, the Privy Council review underlined the overriding importance of continuing to meet a specified set of “operational requirements” necessary for public protection and national security.

As the Home Secretary made clear in his Written Ministerial Statement of 10 December, it is disappointing that subsequent work on the intercept as evidence (IAE) model recommended by the Privy Council review established that it would not be legally viable. Proceeding with implementation on this basis would damage rather than enhance our ability to bring terrorists and other serious criminals to justice.

As the Committee notes, the conclusions reported by the Home Secretary are shared by the cross-party Advisory Group of Privy Counsellors<sup>1</sup>, which has overseen the work programme. Their report<sup>2</sup> to the Prime Minister in December 2009 stated that:

*Having seen the results of the work programme, the Advisory Group believes that although the IAE model, developed on the basis of the original Privy Council review, is broadly consistent with the operational requirements, it would not be legally viable. This is confirmed by a recent European Court of Human Rights case<sup>3</sup>. Further, we have also consulted the present Director of Public Prosecutions. While firmly convinced of the evidential value of intercept material, his view is that the IAE model developed would not be legally viable.*

The Government shares the Advisory Group’s view that the potential gains from a workable intercept as evidence regime justifies further work, intended to establish whether the problems identified may be capable of being

---

<sup>1</sup> Comprising the Rt Hon. Sir John Chilcot, the Rt. Hon. Lord Archer of Sandwell, the Rt. Hon. Sir Alan Beith, and the Rt. Hon Michael Howard QC MP

<sup>2</sup> December 2009, placed in the Libraries of the House

<sup>3</sup> *Natunen v Finland*

resolved. It will report the results of this activity to Parliament before the Easter recess.

The Government also reiterates its previous offer to provide the Committee with fuller informal background briefing by officials.

**11. We dispute the claim that the admission of intercept material would lead to vastly increased costs for enforcement agencies and fear that this argument is being put forward to divert attention from the main issues. We would like to see an estimate of what the additional costs have been calculated to be. (Paragraph 39)**

We agree that a legally viable and operationally sustainable model for the use of intercept as evidence could in some cases result in earlier guilty pleas, shorter trials and savings for the criminal justice system. However, as noted at paragraph 37 of the committee report, the Home Office implementation work programme (the findings of which are contained in 'Intercept as Evidence: A Report', Cm 7760, 10 December 2009) also identified substantial implementation costs both for the interception agencies and the wider criminal justice system.

These costs are over and above those of the current interception regime. Systems would need to be enhanced to evidential standards and running costs would rise, reflecting the need for increased monitoring, review and transcription requirements. Similarly, the presentation of intercept material at court would itself often incur some cost. These additional costs are considerably wider in scope and very likely to be greater in magnitude than potential savings at trial from some earlier guilty pleas.

The Government strongly rejects the unsupported claim in the Committee report that cost has been '*put forward to divert attention from the main issues.*'

**12. Other states have adopted the use of intercept evidence without compromising the work of their security agencies so it is clear that a way can be found without impacting on security services too adversely. We suspect that the apparent unwillingness of security agencies to approach this matter in a constructive matter is attributable as much to institutional inertia and a deeply felt cultural reflex as to insurmountable technical barriers. The clear desire of Prime Ministers and the Government to allow the admission of intercept material should not be frustrated by such responses. (Paragraph 41)**

The Government disagrees with the Committee's assessment.

The original cross-party Privy Council review concluded that different legal and operational contexts made overseas examples of limited relevance in assisting implementation in the UK. Indeed, as set out in the Home Office work programme findings ('Intercept as Evidence: A Report', Cm 7760, 10 December 2009), overseas experience is that the operational burdens for the intercepting agencies of IAE are considerable, meaning that intercept can

support fewer investigations and that the use of intercept as an intelligence tool is significantly reduced.

The findings also make clear that none of the countries examined in the course of this work programme or by the Privy Council review has developed the degree of valuable inter-agency co-operation enjoyed by the UK; overseas law enforcement agencies generally have more limited access to sophisticated intelligence agency interception techniques than is the case here. The combination of the ECHR, as reflected domestically in the Criminal Procedure and Investigations Act 1996, and our adversarial court process makes disclosure obligations more onerous in this country than some others. All these factors significantly increase the risk that evidential use of intercept would compromise sensitive techniques or require cases to be dropped in order to avoid doing so. The result could be to undermine the investigations which currently lead to successful prosecutions.

The Government rejects any suggestion that the security agencies have not approached the matter of IAE in a 'constructive' way and the unsubstantiated suggestion that this is due to 'inertia' or 'a deeply felt cultural reflex'.

The Government regrets that the Committee did not give due regard to the views<sup>4</sup> of the cross-party Advisory Group of Privy Counsellors<sup>5</sup> overseeing the work programme, which commended:

*the commitment demonstrated by officials over the course of work to date. This work is complicated and intellectually demanding, and of necessity requires a detailed understanding of the interception business. It has been necessary to rely on expertise drawn from agencies and departments that would otherwise be fully engaged operationally. We have been impressed by their willingness to engage with the problem and the thoroughness of their work.*

**13. While we accept that in many cases the need to maintain national security outweighs the benefit of admitting intercepted material in court, this will not be the case in every situation and there are no good reasons for completely disallowing even the possibility of admitting intercept evidence in court. We are extremely worried that this prohibition is not purely driven by a rational analysis of the costs and benefits. When we last looked at this issue in December 2007 we commented that:**

***We consider it ridiculous that our prosecutors are denied the use of a type of evidence that has been proved helpful in many other jurisdictions ... We can learn from other similar countries, such as the USA and Australia, how to protect our intelligence sources ... It would not be compulsory to use intercept evidence if it were felt that the damage from doing so outweighed the benefit ...***

---

<sup>4</sup> December 2009, placed in the Libraries of the House

<sup>5</sup> Comprising the Rt Hon. Sir John Chilcot, the Rt. Hon. Lord Archer of Sandwell, the Rt. Hon. Sir Alan Beith, and the Rt. Hon Michael Howard QC MP

**We see no reason to revise our earlier conclusions and strongly recommend that the Government immediately introduce legislation allowing the admission of intercept evidence in court. (Paragraph 43)**

It has been and remains the Government's objective to build on the current successful use of interception as intelligence by enabling intercept material to be used as evidence in criminal trials. However, the challenge is to do so while ensuring that the very significant intelligence dividend is not eroded.

It would not be possible to simply 'cherry pick' cases in which intercept evidence might be adduced without wider implications for any trial following an investigation which had made use of intercept material. For the reasons set out in the findings of the work programme the result would be to damage our ability to bring the guilty to justice and to protect the public.

The Government disagrees with the Committee's overseas comparisons for the reasons set out in response to conclusion 12.

The Government reiterates its previous offer<sup>6</sup> to provide the Committee with fuller informal background briefing by officials.

## **CONTROL ORDERS**

**14. In 2006 we supported the introduction of control orders. We believed at the time that they could be used to disrupt terrorist conspiracies and that there would be circumstances in which it would not be possible to charge individuals but where close monitoring of a suspect would be necessary. However, control orders no longer provide an effective response to the continuing threat and it appears from recent legal cases that the legality of the control order regime is in serious doubt. It is our considered view that it is fundamentally wrong to deprive individuals of their liberty without revealing why. The security services should take recent court rulings as an opportunity to rely on other forms of monitoring and surveillance. (Paragraph 48)**

The Government disagrees with the Committee's conclusion that control orders are no longer effective, that the legality of the regime is in doubt and that the regime is no longer viable. The Government notes that the Committee's commentary also contains factual inaccuracies. The Government's position on control orders was set out in detail in its memorandum to the Home Affairs Committee on Post-Legislative Assessment of the Prevention of Terrorism Act 2005 (Cm 7797), which was laid before Parliament on 1 February 2010.

The Prevention of Terrorism Act 2005 makes provision for both derogating and non-derogating control orders. A derogating control order is one that imposes obligations that amount to a deprivation of liberty within the meaning of Article 5 (right to liberty) of the European Convention on Human Rights (ECHR) and would therefore require the Government to derogate from all or

---

<sup>6</sup> Made in correspondence to the Chair of the Committee on 8 December 2009

part of that Article of the ECHR before the order could be made. A non-derogating control order is one in which the obligations imposed do not amount to such a deprivation of liberty.

No derogation from Article 5 has been made in relation to control orders. Only non-derogating control orders have therefore been made. The Government has complied with the various court judgments concerning control orders and Article 5 to ensure that the obligations imposed in control orders are compatible with the right to liberty. As a matter of law it is therefore inaccurate for the Committee to suggest that current control orders 'deprive individuals of their liberty'.

The Committee report is also inaccurate in suggesting that controlled individuals are not aware why they are subject to an order. In the June 2009 House of Lords judgment in *Secretary of State for the Home Department v AF & Others* [2009] UKHL 28 (*AF & Others*), the Lords held that in order for control order proceedings to be compatible with Article 6 (right to a fair trial) of the ECHR, the controlled person must be given sufficient information about the allegations against him to enable him to give effective instructions to the special advocate in relation to those allegations.

The High Court, applying this test in individual control order cases, considers whether disclosure of sensitive material must be made to the controlled person in order to comply with the right to a fair trial on a case by case basis. Where the judge concludes that there is material that it is necessary to disclose in order for the controlled individual to have a sufficient measure of procedural protection, even though disclosure of that information would be damaging to the public interest, the Secretary of State will be put to his election. In other words, the Secretary of State is given a choice whether to disclose the information, or withdraw it from the case. If the latter, the case then proceeds without reliance on that material, or the Secretary of State (or the court) may decide that there is no longer sufficient material on which to uphold the control order. As a result, all control order proceedings will be compliant with Article 6.

The Government has faced and continues to face difficult choices as to how best to protect the public interest following the June 2009 judgment. We have had to balance the importance of protecting the public from the risk of terrorism posed by an individual against the risk of disclosing sensitive material. Disclosing this material potentially reduces the Government's ability to protect the public from a risk of terrorism. Where the disclosure required by the court cannot be made because the potential damage to the public interest is too high (for example if disclosure could put the life of an informant at risk), we may be forced to revoke control orders even where we consider those orders to be necessary to protect the public from a risk of terrorism.

As of 10 December, only two control orders had been revoked and not replaced by a new one as a result of *AF & Others*. In two further cases, control orders have been revoked on Article 6 grounds and new control orders with significantly reduced obligations imposed in their place. The Secretary of State unsuccessfully argued before the High Court in *Secretary of State for the Home Department v BB & BC* [2009] EWHC 2927 (*Admin*) (*BB & BC*) that in such cases Article 6 was not engaged – or, even if it was, the level of

disclosure required in *AF & Others* did not apply. The Secretary of State is appealing. The control orders remain in force – and the effect of the judgment has been stayed – pending the outcome of that appeal.

In all other current control order cases the Secretary of State considers that sufficient disclosure has been or can be made to the individuals to comply with the level of disclosure required in *AF & Others*. Consequently, the Government has concluded that the control order regime remains viable. This is most obviously illustrated by the hand down before Christmas of three High Court judgments upholding individual control orders, the proceedings for which were held in accordance with the requirements of Article 6 following *AF & Others*.

The Government disagrees with the Committee's assertion that control orders are no longer effective. No executive action can entirely eliminate the risk of terrorism. But in some cases control orders have successfully prevented involvement in terrorism-related activity. In others – the majority – they have restricted and disrupted that activity without entirely eliminating it. On the basis of the very comprehensive classified material to which he had access, Lord Carlile concluded in his 2009 report on control orders that control orders were 'largely effective'. In his 2010 report, Lord Carlile includes some more detailed commentary on effectiveness. For example, he states in relation to three controlled individuals that in each case the order 'has substantially reduced the present danger that exceptionally they still present despite their having been subject to a control order for a significant period of time. Unless control orders were replaced by some equally disruptive and practicable system, in these cases the repeal of control orders would create a worryingly higher level of public risk.'

The Government notes the Committee's suggestion that instead of control orders other forms of surveillance and monitoring should be relied on. Viable alternatives to control orders that offered similar levels of assurance of a controlled individual's location, such as surveillance, would be considerably more expensive. Moreover, passive monitoring is qualitatively different from a control order. A control order disrupts terrorism-related activity. A curfew confines an individual to his house, limiting what he can do for those hours (in conjunction with other control order obligations), and the impact of the curfew goes beyond the hours for which it is in place. Control orders can also have other disruptive obligations in place at all times, regardless of the length of curfew – such as a geographical boundary restricting movement, prohibition on contact with specified individuals, and prohibition on the use of communications equipment. Such disruptive action, often considered vital if we are sufficiently to manage the terrorism-related risk posed by these individuals, is not achieved by solely watching and listening.

Wherever possible we will prosecute suspected terrorists. Where we cannot prosecute, and the individual concerned is a foreign national, we will seek to deport them. Control orders are an effective disruptive tool for dealing with suspected terrorists whom we cannot prosecute or deport. Moreover, control orders are an important means of preventing travel abroad by suspected terrorists.

The Government notes that the introduction of intercept as evidence would not remove the need for control orders. The 2008 Privy Council review noted that it had 'not seen any evidence that the introduction of intercept as evidence would enable prosecutions in cases currently dealt with through control orders.'

In his 2010 annual report on control orders, published on 1 February, Lord Carlile states that: 'it is my view and advice that abandoning the control orders system entirely would have a damaging effect on national security. There is no better means of dealing with the serious and continuing risk posed by some individuals.' He emphasises that he has 'considered the effects of the Court decisions on disclosure. I do not consider that their effect is to make control orders impossible.'

In the light of the Government's conclusion that the control order regime remains necessary and viable, the draft order for renewal of the powers under sections 1 to 9 of the Prevention of Terrorism Act 2005 was laid before Parliament on 1 February 2010.

## **FUNDING**

**15. That the United Kingdom faces a grave threat from terrorism cannot be disputed; we are therefore pleased that budgets for both counter-terrorism policing and the security services have increased substantially.**

We welcome the Committee's recognition both of the seriousness of the threat faced by the United Kingdom and of the substantial increase in resources to counter-terrorism policing and to the Security Service that the Government has made in recent years.

**16. By ring-fencing counter-terrorism budgets, we are concerned that the Government is suggesting that counter-terrorism policing can be "segregated" from other areas of Police work. There is an implicit danger that by marking out counter-terrorism policing as somehow "different" from other activities, specialist counter-terrorism units lose the local link which Assistant Commissioner Yates, and others, rightly prize.**

Ring-fencing of counter-terrorism budgets helps to ensure that adequate resources are made available at a local level to tackle issues that often impact at a national level. Managing funds in this way enables us to reflect changing requirements by adjusting our funding accordingly. For example funding for the protection of the Critical National Infrastructure (CNI) changes from year to year to reflect changes in the assessment of impact should the site be lost, changes in the threat level and changes in the level of response required in respect of different threat assessments. Without the ring fence, local forces would need to increase and decrease the resources they devote to counter-terrorism without receiving a corresponding change in government funding, directly impacting on their ability to respond to other local issues.

Counter-Terrorism is a priority for the Police across the country so it is right that Police Community Support Officers, for example, provide part of our response. We supplement this by providing ring-fenced funds to support additional dedicated resources to work on Counter-Terrorism which complement the contribution made by officers across the Police.

The ring-fencing of budgets in no way segregates counter-terrorism policing from local policing. Indeed, we regard the link “local link” as an important aspect of our approach. Whilst we have established a network of regional Counter-Terrorism Units (CTUs) and Counter-Terrorism Intelligence Units (CTIUs) that work together and are coordinated centrally, these units are located within local Police Forces and work closely with their colleagues in mainstream policing. In addition, we are working with the Police to provide training and advice to a wide range of Police Officers as Neighbourhood Policing is integral to local delivery of many aspects of our strategy, particularly *Prevent*.

**17. We suggest that the Intelligence and Security Committee or the newly-formed Joint Committee on the National Security Strategy would be better suited than a committee of the Association of Police Authorities to take responsibility for providing Parliamentary oversight of all counter-terrorism spending and that this Committee should Report to the House on a regular basis.**

The Committee’s assertion that oversight of Police counter-terrorism funding is limited to that provided by a Police Authority committee is incorrect. The Committee’s recommendation appears not to take account of the range of governance and scrutiny arrangements which are already in place. They are summarised at pages 142/143 of the 2009 CONTEST strategy.

The Home Office – both in terms of Ministers and senior officials – is already accountable to Parliament for the efficient and effective use of the specific grant funding used to support the development of counter-terrorism policing. In support of this there are governance arrangements in place, reflecting the existing tripartite nature of Police accountability in this country, to ensure proper oversight of this funding and its fit with delivery of the overall CONTEST strategy. Senior level boards have been established by the Home Office and ACPO (TAM) to provide complementary avenues of scrutiny.

The Government has worked closely with ACPO(TAM) to improve internal Home Office and Police service control mechanisms relating to Police counter-terrorism funding (through, for example, the establishment of memoranda of understanding in respect of individual grants; performance management arrangements; improved scrutiny of business cases to inform funding decisions). In addition, individual Police Authorities are responsible for scrutinising the use of grant monies in line with their statutory responsibilities.

The Joint Counter-Terrorism Oversight Group (a collection of Police Authorities representing areas with CTUs and CTIUs) was established to co-ordinate oversight of CT spend and ensure lessons learned in one geographical area were being shared with others. The Government supports that initiative. The Group is briefed by the Police and attended by OSCT.

**18. We were told that MI5 has reconsidered the shift in its budget from Northern Ireland terrorism to deal with the threat from Islamic extremists. We welcome this reappraisal but note it illustrates the risks inherent on prioritising threats from different sources.**

It would not be appropriate for us to comment in detail on this specific point which is a matter for the Intelligence and Security Committee who, under the Intelligence Services Act 1994, have responsibility for examining the policy, administration and expenditure of the Security Service.

However, the Government does believe that it is entirely right and proper that resource allocation is regularly reviewed to take account of the evolution of the threat and to ensure that value for money is being achieved.

**19. We remain firmly of the belief that the *Prevent* strand of CONTEST, and engaging local communities in the fight against terrorism, is of the utmost importance. We are encouraged by the way members of all communities have cooperated with the authorities in exposing those individuals who plan to resort to violent extremist methods.**

The Government welcomes the Committee's comments on the importance of the *Prevent* strand of CONTEST, and its recognition of the contribution which members of all communities have made to dealing with those who would resort to violent extremism and terrorism.

*Prevent* remains a relatively new programme in an innovative area in which we and our delivery partners will continue to learn. Nonetheless we have taken it forward quickly and good work has been done. The partnership and information systems introduced in 2008/09 are coming on stream; referral systems are in place; new interventions for vulnerable individuals are being started; a national training pack is being rolled-out; Police capacity has increased; links are being made between *Prevent* in the UK and internationally; many government departments are now actively engaged in delivery, including the FCO, and most recently the Department of Health.

The infrastructure for delivering *Prevent* at a local level is established. Community groups and individuals have become more engaged in *Prevent* and more confident in standing up publicly against violent extremism. OSCT and CLG issued revised guidance on *Prevent* to local partners in June 2009 which built on learning from the previous year. Guidance has also been given on self-assessments against NI35.

The *Prevent* agenda is now part of day to day business for local government and high risk areas have had specialised support. Partnerships and programmes of action are in place in all the priority areas. 73% of areas which do not get *Prevent* funding have partnerships in place and 45% have a programme of action. Using funds from CLG, local authorities have provided assistance to over 1000 community projects intended to produce *Prevent* outcomes. Police *Prevent* capacity has been built up rapidly over the last two years: there are now over 300 dedicated Police posts in place. OSCT and CLG delivered a third highly successful National *Prevent* Conference in

Birmingham in December 2009. Over 1,000 local, national and international partners attended to discuss *Prevent* and to share best practice.

We have developed methods for sharing information on radicalisation more widely than has traditionally been the case with those who are involved in working to counter it. In response to requests from local partners for better information, Counter-Terrorism Local Profiles have been made available. Analysis shows that over 80% of partners surveyed found the CTLP briefing relevant.<sup>7</sup>

The Channel project now operates across 12 Police forces and over 75 Local Authorities. Just over 200 people have been through Channel and been referred mainly for non-law enforcement interventions (including mentoring and pastoral support).

A *Prevent* training package has been developed and is being rolled-out. More than 400 frontline professionals have been trained already and many more will be. Work continues to adapt the package for specific areas: a version has been developed specifically for frontline health professionals.

We are developing work on dealing with the internet as a tool for radicalisation. On 1 February we launched a webpage on Directgov, providing guidance on steps which can be taken by members of the public who have concerns about terrorist, violent extremist or hate crime related content on the internet. The webpage provides advice as to action they can take with internet providers regarding undesirable material. The webpage includes a new online reporting mechanism for members of the public to submit to the Police the web addresses of material they believe to be unlawful. The reports will be processed and actioned by a new national unit within ACPO (TAM) in accordance with powers provided under section 3 of the Terrorism Act 2006,

We have established an extensive programme of domestic and international communications campaigns which both challenge terrorist ideologies and support debate in a wide range of contexts. In doing this we draw on original research which has given us an unprecedented understanding of our audiences.

We will continue to evolve our work on *Prevent* on the basis of our developing understanding of the nature and process of radicalisation, adapting our response to the changing threat.

## **PARLIAMENTARY SCRUTINY**

**20. The Parliamentary Committee on the National Security Strategy was first proposed by the Prime Minister in October 2008. It was not until 13 January 2010 that this Committee was actually established. While we welcome the establishment of this body and we are glad to see our Chairman nominated to serve on it, we feel that this does not inhibit us**

---

<sup>7</sup> Source: IPSOS MORI: Information Sharing Scheme – Evaluation and Development: January 2010

**from further scrutiny of Project CONTEST as the need arises. We also question why this process has taken over a year to complete and suggest that it shows a lack of urgency on the Government's part. (Paragraph 56)**

We are pleased that the Committee welcomes the establishment of the Joint Committee on the National Security Strategy (JCNSS) and we agree that this should not inhibit the HAC from further scrutiny of CONTEST as appropriate within its remit. Following publication of the First National Security Strategy, the Prime Minister consulted widely on the role and membership of the Committee and sought to take on board as many of the points raised as possible before it was established. Since that time, the establishment of the Committee has been subject to the usual channels and Parliamentary processes of both Houses. The final motion to establish the JCNSS was agreed by the House of Lords on the 1st February 2010. The inaugural meeting of the JCNSS will be held on the 9th February 2010.

**21. Changes in the threat level should be explained to Parliament at the earliest practicable opportunity and Ministers should seek to explain their decision in front of a Parliamentary Committee. As well as announcing the change in the threat level, as far as possible Ministerial statements should include how this change will impact on the public. We therefore welcome the attendance of Lord West in front of this Committee on Tuesday 26 January to discuss the change in threat level.**

Threat levels are not decided by Ministers (as the Committee suggest) but by the Joint Terrorism Analysis Centre (JTAC). JTAC make the decision independently of Ministers considering all relevant intelligence and information, and a broad range of factors including the currently assessed intent and capabilities of international terrorist groups. The Intelligence and Security Committee is able, under the Intelligence Services Act 1994, to examine this matter further.

We agree with the Committee that changes in the UK Threat Level from international terrorism should be communicated to Parliament at the earliest practicable opportunity. That is precisely what we have done whenever the Threat Level has changed. However, as threat levels are an important tool for security practitioners working across different sectors of the Critical National Infrastructure, Government Departments and the Police the priority has to be communicating this information to them.

Threat levels in themselves do not require specific responses from the public-who we would urge to remain vigilant at all times.

**22. During this inquiry we have often heard suggestions for reforms to the counter-terrorism structure rebuffed because "it works well at the moment", or "the benefits are not yet proven". There may well be salience to these remarks but it also gives us the impression that a degree of institutional inertia has set in and those involved in counter-terrorism may be willing to settle for existing sub-optimal solutions, rather than proactively reforming to meet ever-changing threats. Time and time again we have been struck by how long it has taken to establish apparently much-needed measures such as the regional**

**counter-terrorism units and the Office of Security and Counter-Terrorism. While the structures that we now have in place may be suitable for combating the terrorist threat as currently constituted we are not confident that government institutions have the desire to constantly adapt to meet ever-changing threats.**

We welcome the Committee's conclusions that the structures now in place are suitable to address the current terrorist threat. However, we strongly dispute the suggestion that they are unable to adapt as that threat evolves in future. We concur with the judgement of the Home Affairs Committee's own counter-terrorism sub-committee in its report of 7 July last year: "the UK's counter-terrorism apparatus is first-class, effective and as 'joined-up' as any system of government can expect".



information & publishing solutions

Published by TSO (The Stationery Office) and available from:

**Online**

[www.tsoshop.co.uk](http://www.tsoshop.co.uk)

**Mail, Telephone, Fax & E-mail**

TSO

PO Box 29, Norwich, NR3 1GN

Telephone orders/General enquiries: 0870 600 5522

Fax orders: 0870 600 5533

E-mail: [customer.services@tso.co.uk](mailto:customer.services@tso.co.uk)

Textphone: 0870 240 3701

**The Parliamentary Bookshop**

12 Bridge Street, Parliament Square

London SW1A 2JX

Telephone orders/General enquiries: 020 7219 3890

Fax orders: 020 7219 3866

Email: [bookshop@parliament.uk](mailto:bookshop@parliament.uk)

Internet: <http://www.bookshop.parliament.uk>

**TSO@Blackwell and other Accredited Agents**

**Customers can also order publications from:**

TSO Ireland

16 Arthur Street, Belfast BT1 4GD

Tel 028 9023 8451 Fax 028 9023 5401

ISBN 978-0-10-177882-4

