Government Response to the Intelligence and Security Committee's Annual Report 2008–2009

Presented to Parliament by the Prime Minister
by Command of Her Majesty

March 2010

Cm 7808

£5.50

ISBN: 978-0-10-178082-7

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

ID 2349641 03/10

Printed on paper containing 75% recycled fibre content minimum.

GOVERNMENT RESPONSE TO THE INTELLIGENCE AND SECURITY COMMITTEE'S ANNUAL REPORT

2008–2009

The Government is grateful to the Intelligence and Security Committee for providing independent and effective parliamentary oversight of the intelligence and security Agencies and for producing its latest Annual Report.

The Committee's report contains a number of conclusions and recommendations. These are set out below (in **bold**), followed immediately by the Government's response.

Redactions are indicated by *** in the text.

A. The Committee considers it essential that the Agencies are able to consolidate the gains they have been able to achieve in recent years in terms of resources and capability. We would be concerned if the Agencies were to suffer real-term cuts in the short or medium term.

The Government notes the Committee's comments. The Government recognises the current delivery pressures on the Agencies (many of which are reflected in the Committee's report) and the impact of the pace of change in technology. These, and other pressures, will require the Agencies to make significant investments in order to maintain their capabilities and consolidate the recent developments. In the current financial climate, however, it is likely that this will mean some difficult choices ahead.

B. It is essential that Government Communications Headquarters signals intelligence capability is maintained and indeed strengthened through its Signals Intelligence Modernisation Programme. However, given the considerable sums of money involved, it is also essential that the work is effectively overseen. We welcome the fact that GCHQ has now introduced improved contract management mechanisms.

The Government welcomes the Committee's recognition that GCHQ's technical investment programme (SIGMOD) is critical to the maintenance of signals intelligence capability in a rapidly changing digital world. GCHQ continues to put considerable effort into refining programme governance in order to allow for agile and rapid delivery as well as for robust financial and project oversight. GCHQ welcomes the Committee's recognition of recent improvements to contract management.

C. The Committee had previously been told that it was "very unlikely" that GCHQ would ever be able to meet the performance targets agreed with the Security Service. We are therefore reassured that GCHQ now believes it is able to meet Security Service key requirements.

The Government welcomes the Committee's comments. GCHQ continues to work closely with Security Service operational and investigative teams. In the last year, GCHQ has provided close support to the Security Service on its highest priority counter-terrorism operations. The ability of GCHQ to understand the Service's detailed requirements, and to respond rapidly in redeploying its efforts as key priorities change, has been fundamental to this success.

D. The potential threat posed to the UK Government, Critical National Infrastructure and commercial companies from electronic attack is a matter for concern. We have heard from our American and Canadian counterparts that they treat this threat very seriously, and we recommend that the UK accord it a similar priority and resources.

The Government agrees with the Committee that the threat to the UK from electronic attack is a matter for concern. The Cyber Security Strategy of the United Kingdom, published in summer 2009, set out the threat and the Government's intended response. Part of this response was to create two new organisations, the Office of Cyber Security (OCS) within the Cabinet Office, and the Cyber Security Operations Centre (CSOC) hosted by GCHQ in Cheltenham. Both bodies were established in September 2009 and have been tackling early priority areas in support of the Cyber Security Strategy of the United Kingdom. OCS provides strategic leadership and cross-government coherence in this area, and CSOC co-ordinates significant cyber security incident response, enables a better understanding of attacks and provides improved advice and information about the risks.

The Centre for the Protection of National Infrastructure (CPNI) also works closely with OCS and CSOC in this field. It provides advice to businesses and organisations across all sectors of the UK's Critical National Infrastructure, helping to mitigate risk and reduce vulnerability to threats in the cyber domain. It also provides them with warnings, alerts and assistance in resolving serious IT security incidents. CPNI has a further "response" function: it is available 24/7 to act as a reporting point for UK companies with concerns about potential national security threats, including cyber attack.

E. The Committee considers that this formerly cavalier attitude towards valuable and sensitive assets was unacceptable. GCHQ must ensure that it controls, tracks and monitors its equipment effectively. Now that proper processes have been introduced, we trust that this problem will not arise again.

The Government accepts the Committee's criticism and concedes that GCHQ was unable to account fully for all of its laptops. However, GCHQ has no evidence of any loss of laptops or classified information. The most likely explanation in most cases is that the laptops were destroyed but without the destruction being fully recorded. GCHQ has now tightened up its controls, which will significantly reduce the risk of any loss of laptops or of any sensitive data they may contain.

F. The attacks in Northern Ireland in March 2009 have shown that the threat from dissident republican terrorism remains very real. While the overall intelligence assessment was accurate, and the threat level was at an appropriate level, *.**

The Government notes the Committee's interest in the intelligence picture in Northern Ireland and shares its concern about the increased threat of attacks from dissident republicans. Significant efforts are being made by the Security Service and other organisations in Northern Ireland, including the Police Service of Northern Ireland, to mitigate this threat.

G. We accept the view of the Security Service that ring-fenced funding would limit its operational flexibility. However, as we stated last year, we are still concerned that counter-espionage is not sufficiently resourced in light of the levels of hostile foreign activity in the United Kingdom. This is a serious threat that must not be overlooked.

The Government welcomes the Committee's acceptance that ring-fenced funding would limit the Security Service's operational flexibility. The Service's overall budget is set as part of the Single Intelligence Account and, as with the other Agencies, annual negotiations about its budget take into account all its operational requirements, including countering the espionage threat. The Service continually monitors the threat in all operational areas and can reprioritise quickly, as its recent reinforcement in Northern Ireland to counter the dissident republican threat has shown.

H. This is the second year in a row that the Secret Intelligence Service has failed to manage its capital spend across the financial year, putting both efficiency gains and value-for-money gains at risk.

The Government notes the Committee's comments. The Secret Intelligence Service is delivering the efficiency savings and gains to which it is committed under the Comprehensive Spending Review 2007. Many of these come from obtaining best value in procurement. The Government notes that the National Audit Office has looked carefully for evidence that spending late in the year has led to poor value, but has found none.

I. The Committee remains concerned that work to address this important challenge is not being adequately resourced.

The Government recognises the importance of this target, and the Secret Intelligence Service has increased the resources allocated to it. The case for further increases will be considered carefully in the context of the need to allocate an appropriate level of resource to the other high-priority issues highlighted in the Committee's report.

J. While the Secret Intelligence Service has made a step change in recent years in terms of staff numbers, the benefits have yet to be seen in terms of an increase in operational capability. It has recognised the need to adapt its established procedures – for example on terms of overseas deployment and training of new entrants – and we hope that this will begin to yield results soon.

The Government recognises the importance of the Secret Intelligence Service evolving its procedures to convert growth into operational capability. Steps have been taken to address this issue, but progress is not expected to come quickly, because the impact of growth will depend on the time required for new officers to gain sufficient experience to realise their full potential.

K. The loss of Secret Intelligence Service data and its subsequent appearance on eBay represent a clear breach of data security procedures, combined with a lack of adequate guidance and enforcement. Although this happened some years ago, the Committee is nonetheless disappointed that data was not being handled securely.

The Government accepts the Committee's conclusion. However, as the Committee has noted in its report, the Secret Intelligence Service's data-handling procedures have been reviewed since this legacy incident occurred in order to mitigate the risks of future losses, although those risks can never be eliminated entirely.

L. Effective and regularly tested business continuity plans are essential for all organisations. We recognise that progress is being made, but remain concerned that there are still vulnerabilities in the plans of all three Agencies. We shall examine these further.

The Government agrees with the Committee on the importance of the Agencies having effective business continuity plans, and welcomes its intention to examine this issue further. As the Committee notes, a great deal of progress has already been made, but the Agencies acknowledge that there are still areas for strengthening their business continuity arrangements. Work continues to ensure that appropriate and effective measures are in place.

M. Both parties would therefore benefit from a discussion as to how to refine the system with regard to the police.

The Government notes the Committee's views. As has been explained to the Committee, the DA-Notice system does not extend to police operations as such, but the Defence Press and Broadcasting Advisory Committee (DPBAC) has already begun to discuss how best to ensure that the system operates effectively in cases where joint police/Security Service operations involve sensitive national security considerations.

N. The Committee recognises that the DPBAC has done, and continues to do, some good work in providing a means for the media and government sides to talk in confidence with a view to protecting information that may prove damaging to national security.

O. Nevertheless, the Committee considers that, as with any system, there is room for improvement and a need to evolve, to ensure that it remains fit for purpose and abreast of changes to the structures and organisations it deals with. We have seen how sensitive the media are when it comes to suggesting change in this area, but we must emphasise that change does not inevitably mean legislation or regulation and that there is room to build on what has gone before and create a more practical and useful system for all those who use it. We recommend that both sides should seriously consider how to move forward on the difficult issues raised here.

The Government notes the Committee's views. The Government accepts that, within a necessarily voluntary system, there is always room for improvement. The DPBAC will continue to keep under review the arrangements for guiding the media and the five standing DA-Notices to ensure that they remain fit for purpose and relevant in a rapidly changing environment. As part of this, the DA-Notice Secretary has been tasked to examine similar systems in other countries, assess mechanisms and concepts which might be relevant to the DA-Notice system and report back to the DPBAC with recommendations.

P. The PREVENT strand of CONTEST is crucial if we are to counter the long-term terrorist threat. While the results of this work may take time to be seen, it has now been two years and we would have hoped that progress could by now be evaluated against more quantifiable outcomes. We therefore recommend that more effective measures are developed against which to assess progress.

The Government welcomes the Committee's recognition of the importance of PREVENT in our work against international terrorism. PREVENT is a long-term strategy that seeks to stop people from becoming terrorists or supporting violent extremism. As the Committee recognises, the effects of the PREVENT strand of CONTEST will only be seen in the long term. However, the Government will continue to devote effort to developing measures for evaluating the effectiveness of PREVENT, covering the full range of national and local partners who are now engaged in the delivery of the strategy.

Q. The slow progress in establishing the National Security Forum appears to have had a negligible impact on the other elements of the national security machinery (including the strategy itself, the Agencies, and the Ministerial Committee on National Security, International Relations and Development). We therefore question whether the National Security Forum is in fact a necessary part of the National Security Strategy machinery.

The Government notes the Committee's views but remains committed to the interim National Security Forum and the establishment of the permanent Forum. The Prime Minister announced the establishment of the interim National Security Forum on 9 March 2009. Since then, the Forum has met on seven further occasions (three of which fall within the period covered by this Annual Report). This is in line with the Prime Minister's intention for the Forum to meet around six times each year.

The National Security Forum has discussed a range of topics, including the national security implications of the economic downturn, the national security implications of energy security and the UK's approach to maritime security. Forum advice is formally submitted to the Ministerial Committee on National Security, International Relations and Development, and has contributed significantly to the development of the annual update of the National Security Strategy and the Cyber Security Strategy of the UK. The Prime Minister himself has been present at Forum discussions on a number of occasions, emphasising the value he places on the Forum's advice.

In his written ministerial statement announcing the establishment of the interim Forum, the Prime Minister explained that the Government would report publicly each year on the Forum's work, and we expect the first such report to be made in March 2010.

R. The Committee does not accept the Government's response to our recommendation made last year, nor do we approve of the changes that have been made to the Professional Head of Intelligence Analysis (PHIA) role, which directly contradict our recommendations. We reiterate that the PHIA, established as a result of the Butler Inquiry, must have a distinct and separate role.

The role of the Deputy PHIA remains distinct and separate from the assessment process. The position of the Deputy PHIA is broadly the same as the role of the previous PHIA, who also reported to the Joint Intelligence Committee (JIC) Chair. In raising the role of PHIA to Permanent Secretary level, the Government sought to reflect the seriousness with which the position is regarded. The change does not impact the day to day work of the team.

S. We welcome the fact that the "Challenge Team" in the Joint Intelligence Organisation has been moved from the Head of the Assessments Staff to the Deputy Professional Head of Intelligence Analysis (PHIA). However, as the PHIA post has now been subsumed within the JIC Chair, the team's independence has not, in reality, been increased. The JIC Chair is now performing the role of both "gamekeeper" and "poacher", undertaking a challenge function in relation to his own work. This reinforces our earlier view that the PHIA must be a separate and distinct role.

As the Committee notes, the Challenge Team has been moved from the Assessments Staff to the Deputy PHIA in order to increase its independent role. The Deputy PHIA is in the best position to objectively challenge the conclusions made by the Assessments Staff. The suggestion that the PHIA has been "subsumed" within the role of JIC Chair is incorrect. While it is true that the same individual holds both positions, the roles are distinct and can be performed in parallel without damaging the independence of the Deputy PHIA or the seriousness with which the challenge function is taken. The Deputy PHIA attends JIC meetings and is able, if neccessary, to challenge assessments or conclusions at all levels.

T. The Committee remains concerned that these reductions in Defence Intelligence Staff (DIS) staff numbers will have a serious impact on DIS capability. They could also have long-term implications for DIS core customers and the wider intelligence community.

The Government notes the Committee's concerns. Careful prioritisation of analytical effort and consultation with DIS customers within and beyond the Ministry of Defence will remain key to ensuring that DIS continues to respond to priority requirements and maintain capability for the longer term.

U. We had hoped to include in this Report a detailed account of the Cabinet Office's decision to abandon Phase 2 of the SCOPE programme. However, the Committee is still investigating the circumstances surrounding the decision, and commercial and legal negotiations between the Cabinet Office and contractor continue. We will therefore report on this matter in our next report.

The Government notes the Committee's comments. The Cabinet Office is continuing to work towards resolving the issues arising from the termination of the programme. The aim of the work is to ensure that the Government and the taxpayer recover from the supplier the appropriate value relating to those undelivered parts of the programme. The Government will report the outcome of this work to the Committee in due course.

V. CLiC appears to be progressing well so far. We are optimistic that it will deliver some of the IT solutions that the (far more costly) SCOPE Phase 2 programme was unable to. It is regrettable that this same practical and incremental approach was not adopted in the planning of the SCOPE programme.

The Government notes the Committee's findings. Work on CLiC (Collaboration in the Intelligence Community) continues to progress well. The incremental approach that has been adopted is delivering results at a relatively low cost and with manageable risk levels. The Government intends to continue with this incremental approach to enhancing intelligence-sharing capabilities.

W. While the then Prime Minister's specific assurances to this Committee, in relation to Diego Garcia, were on the basis of firm assurances from the United States, these recent developments have demonstrated that the UK must be more robust in verifying such assurances in the future.

The Government has been robust in verifying such assurances, and will continue to be so. The Government acknowledges the importance of verifying assurances in circumstances where new information comes to light. As the Committee noted, we did this with the US following the new information that came to light in February 2008 about the use of Diego Garcia. Nevertheless, the Government believes that we must avoid proceeding with our bilateral partners on the basis of mistrust or a presumption of deceit, and must instead make considered judgements on the basis of careful analysis and foreign policy expertise.

X. We regret that neither the Security Service nor the Secret Intelligence Service identified the relevant documentation in response to Committee requests or in support of evidence given to us by their respective Heads during our original rendition inquiry. There is no convincing explanation as to why this information was not made available to this Committee. While we do not believe that this was a deliberate attempt to deceive us, it highlights fundamental problems with the record-keeping systems and processes of both Agencies.

The Security Service and the Secret Intelligence Service briefed the Committee in considerable detail during its rendition inquiry. It is regrettable that some relevant documentation was not provided to the Committee at the time. However, this documentation was passed to the Committee as soon as possible following its identification and, as the Report notes, there was no intention to mislead the Committee. Significant resource is being dedicated, within both organisations, to improve record keeping and information management.

Y. While we understand that the balance of the Agencies' effort must be focused on operational work, at the same time good record keeping is crucial. The Agencies' operational work is about knowledge and information, and the ability to retrieve such information is central to the work with which they are charged. We welcome the assurances we have received from the Security Service and the Secret Intelligence Service that they are taking action to rectify the problems with their records, although we note that it will take several years before new systems are fully established. This has serious ramifications – both in terms of the Agencies' own work and for the reliability of the evidence they submit to this Committee.

The Government agrees that good record keeping is crucial to the work of the Agencies. As mentioned above, considerable resource is being devoted to improvements in this area. These are significant and important projects which, as the Committee notes, will take time to implement fully; however, improvements are ongoing.

Z. The Committee considers that continued investment in the Agencies' capability to access communications data and undertake lawful interception is essential to the national security of the UK.

The Government welcomes the Committee's findings. The Government continues to work closely with the Agencies and with industry with a view to ensuring that the Agencies' capabilities continue, and to bring forward necessary legislation at a future date.

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

Online
www.tsoshop.co.uk

Mail, Telephone Fax & E-Mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
E-mail: 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
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
028 9023 8451 Fax 028 9023 5401

ISBN 978-0-10-178082-7

9 780101 780827