Government Response to the Intelligence and Security Committee's Annual Report 2012-2013

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

17 October 2013

Cm 8736 £6.25

Any enquiries regarding this publication should be sent to us at
Cabinet Office, 70 Whitehall, London, SW1A 2AS.

ISBN: 9780101873628

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

ID 2597695 10/13

Printed on paper containing 75% recycled fibre content minimum.

GOVERNMENT RESPONSE TO THE INTELLIGENCE AND SECURITY COMMITTEE'S ANNUAL REPORT 2012-2013

The Government is grateful to the Intelligence and Security Committee ("the ISC") for its continued independent and effective parliamentary oversight of the intelligence and security Agencies ("the Agencies") and for producing its most recent Annual Report. The ISC's report contains a number of recommendations and conclusions. These are set out below (in **bold**); each recommendation/conclusion is followed immediately by the Government response.

A. Despite the increased profile of other threats such as cyber security, counter-terrorism work rightly remains the primary focus of the intelligence and security Agencies. Their work in analysing intelligence to understand the threat and seeking to help to prevent attacks remains crucial to our national security.

A1. The Government agrees with the ISC that counter-terrorism work remains the primary focus of the intelligence and security agencies, and that this work remains crucial to our national security. Terrorist threats to the UK and UK interests come from both international and Northern Ireland-related terrorism. A significant proportion of Agency resource remains directed towards countering the terrorist threat, enabling the Agencies to focus on this important work whilst also understanding and mitigating the threat in other key national security areas, such as cyber, hostile foreign activity and counter proliferation.

B. The shape of the terrorist threat is potentially changing from tightly organised cells under the control of structured hierarchies to looser networks of small groups and individuals who operate more independently. It is essential that the Agencies continue to make a clear assessment of this evolving picture in order to keep ahead of the threat and to help to prevent attacks and loss of life.

B1. The Government agrees that it is crucial that the Agencies continue to make a clear assessment of the evolving terrorist threat to help prevent attacks and loss of life. The nature of the threat may be changing from tightly organised cells with structured hierarchies to looser networks of small groups and individuals operating independently, but it is also diversifying as Al Qaeda and its affiliates expand into a wider range of countries and seek to exploit permissive operating conditions to facilitate attacks on the UK and UK interests. The Government also agrees that lone actors and self organised groups pose a threat; the Agencies will continue their work to identify and disrupt the terrorist threat, whatever form it takes.

C. The Committee shares the concerns of the Independent Reviewer of Terrorism Legislation over what happens when individual Terrorism Prevention and Investigation Measures (TPIMs) come to the end of their two-year limit. The Government must take steps now to ensure that they have sufficient policies in place when TPIMs have reached their limit and cannot be extended.

C1. The Government will never put national security at risk. The two-year limit for TPIM notices demonstrates our belief that such measures should not be imposed indefinitely on individuals who have not necessarily been convicted of a criminal offence. Both the current Independent Reviewer, David Anderson QC, and his predecessor Lord Carlile have expressed support for the two-year limit.

C2. Individuals who are assessed to pose a terrorist threat – including those who are, or have been, subject to TPIM notices - are investigated by the Security Service and the police. Government Officials work closely with the Security Service, police and other agencies to ensure an appropriate response to those subject to TPIM measures. Particular attention has been paid to ensure that appropriate arrangements are in place at the expiry of those measures. These include keeping subjects under investigation if necessary, using all the tools available to the police and Security Service, along with the involvement of Prevent officers and the National Offender Management Service to provide support and encourage subjects away from extremism. The police and Crown Prosecution Service (CPS) also keep prosecution under review throughout the duration of the TPIM notice. The TPIM Review Group, involving Government Officials and representatives of the police, Security Service and CPS, meets quarterly to consider the measures in place. The Government has full confidence in the ability of the Security Service and the police to manage any threat posed.

C3. The ISC noted that a number of breaches of TPIM restrictions had occurred. Breaches are criminal offences and the police monitor closely TPIM subjects' compliance with the measures in their TPIM notice. Since the introduction of TPIMs, there have been two breach prosecutions that have gone to trial, resulting in the conviction of one TPIM subject for three offences. A number of other prosecutions are pending.

D. The threat the UK is facing from cyber attacks is disturbing in its scale and complexity. The theft of intellectual property, personal details and classified information causes significant harm, both financial and non-financial. It is incumbent on everyone – individuals, companies and the Government – to take responsibility for their own cyber security. We support the Government's efforts to raise awareness and, more importantly, our nation's defences.

D1. The Government agrees with the Committee's assessment that the cyber threat to the UK is significant and complex and welcome their support for our response. The first years of the National Cyber Security Programme ("the NCSP") have laid the foundation for the step change in capabilities we need to tackle cyber threats in the UK, making sustained progress against all four UK Cyber Security Strategy objectives.

D2. We have invested in GCHQ's cyber capability and are now better able to detect, understand and combat this threat than ever before. We have strengthened national capabilities to tackle cyber crime by bringing together the Metropolitan Police Service Ecrime Unit and the Serious Organised Crime Agency's law enforcement teams to form the National Cyber Crime Unit ("the NCCU") within the National Crime Agency ("the NCA"). The NCCU combines traditional investigative skills with cyber specific

capabilities and includes dedicated cyber overseas liaison officers to facilitate collaboration with overseas partners.

D3. As the cyber threat knows no boundaries international co-operation is crucial. We have continued to promote the UK's vision of an open, vibrant and secure cyberspace across the breadth of our international activity, both in multilateral organisations such as the UN and within the EU and through our growing network of bilateral relationships.

D4. Cyber threats to our national infrastructure are of particular concern and, together with the Centre for the Protection of National Infrastructure and GCHQ, we have strengthened our defence against cyber threats that could disrupt essential services through unprecedented partnership with industry. This year saw the launch of the Cyber Security Information Sharing Partnership ("the CISP"), providing key companies with a secure forum in which to exchange information on cyber threats and vulnerabilities with the Government and each other in real time. Membership stands at nearly 170 firms, with new firms joining on a regular basis. Cyber Incident Response schemes have also been launched to support a range of organisations that may be victims of cyber attack and provide them with access to government assured, certified providers of response and clean-up services.

D4. Building on the success of these initiatives, this Government will launch the UK's national Computer Emergency Response Team in early 2014. This will further improve national co-ordination of cyber incidents, act as a focal point for international collaboration and extend our incident response support to the wider UK economy as well as the CNI and defence supply chain.

D5. We have worked across the private sector to help companies defend their networks, engaging business on many levels. Following the publication of The Cyber Security Guidance for Business, including the Ten Steps to Cyber Security, in September 2012, a wide range of briefings and seminars with industry groups have taken place as part of our ongoing efforts to raise awareness and help business respond. In addition the Department for Business, Innovation and Skills ("BIS") recently launched the Cyber Governance Health Check which will assess how effectively top FTSE 350 companies are managing cyber risks; is leading a joint Government-industry process to select a preferred organisational standard for cyber security; and has tailored guidance for SMEs which will also be targeted with the general public as part of a NCSP funded national awareness campaign commencing in the next few months.

E. Whilst work is under way to develop those capabilities that will protect the UK's interests in cyberspace, it is now halfway through the Spending Review period, and we are therefore concerned that much of this work remains preparatory and theoretical, with few concrete advances.

E1. The Government notes the Committee's concerns and would reassure the Committee that work is underway in this field. By its very nature, this work is classified and as such cannot be detailed here; however, the Government will continue to brief the Committee as appropriate. The MOD has stated that its aim is to "mainstream" Cyber

within Defence at all levels through the Defence Cyber Security Programme (DCSP), which will run until 2015 as part of the National Cyber Security Programme.

F. Cyber security will continue to be a significant threat beyond the end of this Spending Review period. We are pleased to see that the funding for the National Cyber Security Programme will be extended into 2015/16. However, planning must begin now to ensure that resources will be made available to combat cyber attacks in the latter half of this decade, bearing in mind the resources our allies are putting into this area in recognition of the seriousness of the threat. The Government must ensure that real progress is made as part of the wider National Cyber Security Strategy: the UK cannot afford not to keep pace with the cyber threat.

F1. The Government notes the Committee's concern. The National Cyber Security Strategy provides the basis for the Government's long-term approach, and funding for its delivery is a clear priority: 2013 Spending Review settlement pledged £210m for cyber security in 2015/16, building on the previous four years and £650m of the National Cyber Security Programme funding. These funds will sustain the depth and pace of change, supporting the full range of the UK's cyber ambitions, as articulated in the UK Cyber Security Strategy. The settlement shows the Government's continuing commitment to funding in full the national cyber security effort.

G. The Committee recognises the significant contribution that the Agencies are making to the international efforts regarding Iran's nuclear weapons programme. Such work should continue to receive a high priority. However, we note the challenges posed in gathering intelligence against this particular target.

G1. The Government welcomes the Committee's recognition of the important work the Agencies are undertaking in this challenging area, which will remain a high priority.

H. The support provided by the Agencies and Defence Intelligence to the UK's military operations in Afghanistan has been invaluable. We are, however, concerned that Defence Intelligence's intelligence collection capabilities, which have been built up slowly and at considerable cost to support the campaign, may be easy prey for a department looking to make financial savings. We urge the Government to ensure that these vital capabilities are preserved and to give consideration as to how they can be redeployed when not required in support of combat operations.

H1. The Government welcomes the Committee's recognition of the invaluable contribution that the Agencies and Defence Intelligence have made to military operations in Afghanistan. Although no part of the Defence budget can be entirely immune from financial savings, the MOD will continue to need a range of intelligence collection capabilities post-Afghanistan. We are reviewing the future size and shape of DI's intelligence collection capabilities.

I. The Committee has repeatedly warned of the risks of cutting resources – in particular to Defence Intelligence – to the UK's ability to provide the necessary level of global coverage. Whilst we recognise that burden-sharing arrangements with allies

may offset some of the impact, there must continue to be a critical mass that can respond to unexpected events without this being at the expense of coverage of other key areas. We are concerned that shifting resources in response to emerging events is 'robbing Peter to pay Paul': we must maintain the ability to respond to more than one crisis at a time.

I1: The Government's resources are focused on those areas that matter most to UK national interests. It is not possible and does not provide value for money to have intelligence resources everywhere at all times. Enhanced sharing sharing arrangements are helping Defence Intelligence ("DI") and the Agencies maintain their ability to respond to unexpected events and to plan effectively for contingencies.

J. Closed Material Procedures allow evidence to be heard which, under Public Interest Immunity arrangements, was previously excluded from cases altogether (sometimes leading to the abandonment of proceedings and/or an unavoidable settlement if the Government could not bring evidence in its defence). While CMPs are not ideal, they are better than the alternatives: this is an imperfect solution, but a pragmatic one. Taken together with the Norwich Pharmacal reforms, we consider that the changes should allay the concerns of those allies with whom we exchange intelligence crucial to our national interest.

J1. The Government agrees with the ISC that the provisions of the Justice and Security Act 2013 ("the Act") which allow the use of Closed Material Procedures ("CMPs") in civil cases involving national security material are a practical solution to a very real problem. The same is true of the true of the provisions in the Act which reform the *Norwich Pharmacal* jurisdiction in order that it should not apply in certain circumstances where the information is sensitive. The Government was grateful for the engagement of the Committee during the Act's passage through Parliament which played an important role in determining the shape of the final provisions which were approved by Parliament.

K. The Committee welcomes the real changes made by the new Joint Intelligence Committee Chair, which demonstrate an understanding of how the JIC should operate at the centre of the UK intelligence machinery. Continuous improvements such as these are vital in ensuring intelligence advice to Ministers remains relevant and can respond quickly to changing requirements. We hope that these measures will reinvigorate the JIC and give it a new lease of life.

K1. The Government welcomes the Committee's comments on the positive changes made by the new Chair of the JIC which continues to have a central role in providing advice to Ministers, particularly via the National Security Council.

L. There does seem to be a question as to whether the claimed savings and efficiencies that the Agencies must secure during the Spending Review period are independently verifiable and/or sustainable. The Agencies must ensure that reported savings are real and sustainable. The individual Agency and central SIA finance teams must work together to address the National Audit Office's findings and provide the necessary levels of assurance.

L1. The Agencies remain fully committed to delivering their overall Efficiency targets for the SR10 period. Building on the findings in the National Audit Office report, they continue to refine and strengthen their internal and cross-Agency processes for challenging, validating and reporting savings. Some of these savings relate to the avoidance of investment costs when capabilities can be shared across more than one Agency; since these savings are not sustainable from year to year, the Agencies recognise the imperative in identifying new savings towards the overall target.

M. Whilst we are reassured that some of the savings envisaged under the Corporate Services Transformation Programme (CSTP) will be achieved by other means, we note that the Committee was not kept informed about these changes. Although this was acknowledged to be a high-risk programme, as late as December 2012 – when we last received information on the collaborative savings programme – there was no indication of the trouble CSTP was in, nor of the effort being put into procurement savings. Indeed, we were asked to postpone our own review of the programme. This failure to keep the Committee informed of significant matters within its remit is unacceptable.

M1. The decision by the Agencies to close CSTP was complex and difficult. The Agencies have established an alternative approach for their collaborative work on Finance, vetting and HR functions, implementing lower cost, lower risk initiatives based on process redesign and sharing best practice. The beneficial outputs from CSTP are being taken forward as part of this work. The work to deliver savings through Procurement has always been part of the Agencies' plan: it continues as envisaged and remains central to the overall efficiency agenda. The Agencies recognise the need to keep the Committee informed on such matters.

N. We recognise that during the run-up to the Olympics operational requirements were, rightly, prioritised over efficiency savings but time is running out: we are already over halfway through the Spending Review period in which these savings must be found. It is essential that real and sustainable efficiencies are delivered if front-line capabilities are to be protected. More needs to be done urgently.

N1. By the end of FY2012-13, the Agencies delivered savings which were cumulatively greater than the Efficiency targets set for that period. Principally, these savings were delivered through collaboration on IT and Procurement, plus Agencies' own internal efficiency programmes. Achievement of a significant proportion of the remaining collaborative savings is planned through the development of joint technical capabilities. During the run up to the Olympics, the Agencies focussed on effectiveness through developing and sharing capability; improving productivity and scale; quicker assessment of threats; reducing operational risk; minimising duplication of effort; and ultimately reducing risk of intelligence failure. This work now provides a basis for the Agencies to switch the focus of this collaboration to one that primarily delivers considerable savings.

O. The Agencies have said that they are "fairly confident" that operational capabilities will be protected during the Spending Review period: given the surprising lack of clarity around the collaborative savings programme – an issue that

has such far-reaching consequences – the Committee does not fully share their confidence.

O1. The Agencies are committed to preserving their operational capabilities, enabled not only by the delivery of collaborative savings but also by securing internal efficiencies and by sharing capabilities wherever possible. Every effort is being made to ensure this target is achieved. However, in the unlikely event of the envisaged savings falling short of the SR10 efficiency target, investment in mission capability would be prioritised over investment in corporate areas.

P. Whilst SCOPE Phase 1 was successful, Phase 2 was beset by problems and delays and it is disappointing that it was abandoned. The strict security requirements led to a complex, highly customised secure solution which greatly increased the risk of the project failing. This must be borne in mind, and lessons learned, for future secure IT projects.

P1. The successor to Scope has delivered the capabilities and benefits that were intended to come with Scope Phase 2. The new service has transformed the SIA's ability to share its product quickly and securely, and introduced for the first time secure collaborative working across the intelligence community. The system is used by seventeen Government Departments, with plans for further expansion including the Police. It is also used by twenty-five UK embassies. All this has been achieved for much lower than the anticipated cost of Scope. Additionally the annual upkeep costs of the new system are considerably lower than many lower classification systems being used by government departments. This was achieved by adopting an incremental approach to delivery, simpler governance and delivery structures and also by avoiding overreliance on a single external system provider.

Q. The decision to cancel SCOPE Phase 2 was taken after an 'informal review' outside the normal governance arrangements, reducing accountability and inevitably raising questions over due process. It has since taken three and a half years to bring the Phase 2 project to a close. Whilst the details of the resolution are commercially confidential, we are aware of them and believe this represents a sensible conclusion to what has been a rather sorry saga.

Q1. The decision to discontinue development of Scope Phase 2 was taken by the Scope Oversight Board, chaired by the Senior Responsible Owner for Scope. The Oversight Board was advised by a review informed by external technical experts and legal advisers. Both the technical and legal experts agreed that there was no realistic prospect of the Scope Phase 2 being delivered in any reasonable timescale or at an affordable cost. It was on the basis of this expert advice that the Oversight Board made the decision to stop development of Phase 2 and seek resolution with the supplier. The resolution was satisfactory for government, being essentially cash neutral for the exchequer.

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
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Houses of Parliament Shop
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders: 020 7219 3890/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: shop@parliament.uk
Internet: http://www.shop.parliament.uk

TSO@Blackwell and other accredited agents