Submission to ISC Privacy and Security Inquiry from HMG

1. This submission has been co-ordinated by Cabinet Office on behalf of HMG. It has been agreed by the Security and Intelligence Agencies and the National Crime Agency, and relevant Ministers. The Government will, of course, continue to support the Committee's Inquiry with further evidence and perspectives as required, and looks forward to engaging with the Committee on their conclusions when reached.

Executive Summary

2. The first duty of any Government is the protection of its citizens. For this Government, this responsibility includes protecting the rights of its citizens – including the rights to privacy and freedom of expression, as well as the right to personal safety and right to life. To meet its responsibilities the state has a duty to investigate and counter serious threats to the security of the UK, so that people can go about their business freely and with confidence. Parliament has debated at length the appropriate way in which this should be achieved. It did so when the rules governing the work of the Agencies were brought into law; and more recently during the passage of the Justice and Security Act 2013 which strengthened Parliamentary oversight of how the Agencies work to keep us safe.

3. The consequence of this rigorous Parliamentary process is a robust legal and policy framework that ensures that the work of the Agencies is authorised, necessary and proportionate. The Agencies do not gather or disclose information other than in support of their statutory functions as set out in the Security Service Act 1989 (SSA) and the Intelligence Services Act 1994 (ISA); and in line with their lawful purposes: safeguarding the national security and economic well-being of the UK; and in support of the prevention or detection of serious crime. They work strictly in accordance with Ministerially endorsed priorities. As public authorities for the purposes of the Human Rights Act 1998 (HRA), all three Agencies act in accordance with the requirements of the European Convention on Human Rights (ECHR).

4. Secret intelligence plays a vital role in helping the Agencies keep us safe. Its collection helps them to combat a wide range of diverse and constantly evolving threats to UK national security. Maintaining the secrecy of this information, as well as the methods used to acquire it, in order to counter these threats is particularly important in this internet age. The perpetrators of today's threats can maintain a rapid pace of technological advancements, adapting their capabilities to progress their objectives and evade detection.

5. The Agencies must be able to access information to safeguard UK interests. This access is always carefully considered and authorised at an appropriate level according to the degree of intrusion involved. It is also limited to specific statutory purposes and subject to oversight by Ministers, the Interception of Communications Commissioner and the Intelligence Services Commissioner (the Commissioners), the

Intelligence and Security Committee of Parliament (ISC) and the Investigatory Powers Tribunal (IPT).

6. The Agencies and the Government welcome this oversight. They place great value in public confidence, recognising that without the public's support they cannot fulfil their functions, and continually challenge themselves to provide increased transparency of their activities, where this is lawful and not damaging to national security.

The Threats

7. A fundamental role of the Agencies is to identify, investigate and disrupt threats to UK national security. Today, the UK is facing serious and diverse threats on more fronts than ever before[1]. Broadly categorised, these include:

International Terrorism

8. The UK national threat level from international terrorism is SUBSTANTIAL (an attack is a strong possibility). Al-Qaeda continues to have the intent to conduct mass casualty terrorist attacks against the UK and its interests overseas. Whilst its capability to launch centrally directed large-scale attacks in the West has been degraded, it remains. Of greater concerns is Al-Qaeda's use of its media outlets to encourage its affiliates in the region to conduct large-scale attacks on its behalf. Al-Qaeda inspired but self-organised groupings or individuals have posed the most significant terrorist threat in the UK for the last few years. The killing of Fusilier Lee Rigby in May 2013 was a particularly shocking example of this. Several thousand Islamist extremists are based in the UK with varying degrees of intent and capability to engage in terrorism.

9. The threat to the UK is most pronounced from those individuals who have travelled abroad (particularly, at present, to Syria) to join terrorist groups linked to Al-Qaeda and then returned with the experience and intent to carry out a lethal terrorist attack. Al-Qaeda Core in South Asia continues to pose a threat and its global affiliates still want to attack the UK. Al-Shabaab demonstrated its capability to target Western interests outside Somalia with lethal effect in the Westgate Shopping Centre in Nairobi in September 2013. The attack by Al-Qaeda linked extremists on the In-Amenas oil facility in Algeria in January 2013 was intended to both dissuade Western investment in North Africa and take hostages. The tactic of kidnapping Westerners for ransom is now prevalent in all major conflict zones.

Northern Ireland-related terrorism

10. The threat level in Northern Ireland remains 'SEVERE' (an attack is highly likely). The Northern Ireland-related terrorist threat to the rest of the UK is

[1] As set out in the Government's Counter-Terrorism Strategy, the National Security Strategy, the National Cyber-Security Strategy and the Serious and Organised Crime Strategy.

'MODERATE' (an attack is possible but not likely). In 2013 dissident republican factions continued to reject the political process and carried out 30 attacks on national security targets, all in Northern Ireland. Many of these were unsophisticated though some demonstrated lethal intent. Significant incidents included an attack on a police convoy using automatic weaponry and the planting of an improvised explosive device (IED) under a police officer's car.

*Hostile Foreign Activity and the Cyber Threa*t

11. The UK continues to be a high-priority target for a number of highly-capable foreign intelligence services. These services actively seek to obtain official and commercially sensitive intelligence in their governments' national interests. Whilst the damage from espionage can be difficult to quantify, it is clear that it is extremely harmful to UK national interests. Recent cases illustrate the significant impact an individual can have. In 2012, a Royal Navy submariner attempted to pass classified government information to the Russian Intelligence Services, which had the potential to compromise the UK's nuclear deterrent capability. Following investigation, he was arrested, convicted and sentenced to 8 years in prison.

12. UK Government, technology, defence, security and the commercial sectors are all at risk both from 'traditional' espionage and cyber espionage. It is often very difficult to attribute operations in cyberspace, but we know that there are several established, capable states – as well as determined individuals - seeking to exploit computers and communications networks to gather intelligence, intellectual property and information to enable them to commit large scale financial fraud.

Proliferation of Weapons of Mass Destruction (WMD)

13. The UK continues to support international efforts to prevent WMD proliferation in the Middle East and North Korea. The Agencies play an important role in preventing states of proliferation concern from acquiring technology (tangible materials and intangible knowledge) that would assist state programmes to develop WMD and their means of delivery.

Serious and organised crime

14. The Agencies' have a specific role to act in support of the police and other law enforcement agencies in the prevention and detection of serious crime. Serious and organised crime costs the UK at least £24billion each year. It leads to loss of life and can deprive people of their security and prosperity. Crime groups intimidate and corrupt and have a corrosive impact on some communities. The abuse and exploitation of children has a lifelong and devastating impact on victims. Organised immigration crime threatens the security of our borders. Financial crime undermines the integrity and stability of our financial markets and institutions. Overseas, organised crime undermines good governance and the stability of countries and can facilitate terrorism.

Far-right terrorism

15. The threat from Far-right terrorism is not assessed to be on the scale of international terrorism. But in April 2013, Mohammed Saleem was stabbed whilst walking home from a Birmingham mosque by Paylo Lapshyn, less than a week after Lapshyn had arrived in the UK. Lapshyn, a white supremacist, pleaded guilty to murder as well as plotting to cause explosions near mosques in Walsall, Tipton and Wolverhampton in June and July 2013. He was sentenced to 40 years in prison.

Why secret intelligence is essential to countering the Threats

16. In order to identify, understand and counter the national security threats facing the UK, our Agencies need information. They must be capable of monitoring and then disrupting those individuals and networks posing a threat to the UK but about whom there may be limited or partial knowledge. They must also be able to generate and quickly assess new leads that could reveal emerging threats or identify previously unknown subjects of concern. This involves the amalgamation, analysis and exploitation of a variety of information lawfully obtained from both open and covert sources. This may require the Agencies to sift through ' haystack' sources – without looking at the vast majority of material which has been collected - in order to identify and combine the 'needles' which allow them to build an intelligence picture. In turn, this picture allows the Agencies to make the right connections between disparate pieces of information, ensuring leads are resolved and a depth of knowledge is built quickly on the correct targets, and with minimal intrusion.

17. In recent years, the Agencies have achieved significant success in preventing major terrorist attacks against the UK. This includes the airlines plot in 2006, which aimed to destroy eleven transatlantic airliners in mid-flight simultaneously; the UK network arrested in late 2010 for planning attacks against UK economic targets; and the Birmingham-based group arrested in September 2011 which sought to conduct an attack 'bigger than 7/7' by detonating multiple IEDs. In all these mass-casualty plots the collection of secret information played a vital role in enabling the Agencies to identify and thwart the attackers, and see substantial sentences handed down to them.

18. In Northern Ireland, pressure from the security forces, enabled by intelligence, means dissident republicans are forced to proceed slowly and cautiously if they are to carry out attacks. For every attack which takes place several more are disrupted in the planning stages. There have been cases in the Courts where covert intelligence has enabled the disruption of attack planning, allowing serious terrorist charges to be brought. Similarly, searches guided by covert intelligence have led to the recovery of significant quantities of firearms, explosives and other terrorist materiel.

19. Collection of information relating to the activities of hostile individuals is essential to work countering the threats they pose to cyber security. Lawfully

gathered intelligence provides the basis for the advice provided to Government and private industry about how best to protect themselves against cyber attack.

The legal framework governing access to and use of data

20. While information lies at the heart of the work of the Agencies, there are clear statutory processes governing their access to data and the use to which it can be put. The work of the Agencies is carried out in accordance with a strict legal and policy framework, including the Regulation of Investigatory Powers Act (RIPA), the SSA, the ISA and the HRA. This ensures that all activity is authorised, necessary and proportionate, and that there is rigorous oversight, including from Secretaries of State, the Commissioners, and the ISC.

21. The acquisition, aggregation, usage, sharing and retention of information involve varying degrees of interference with the privacy rights of individuals. The fundamental rule is that the Agencies may only acquire, use or disclose information/personal data where this is necessary for the proper discharge of their other statutory functions, and proportionate to the statutory purpose or objective. The Agencies must always attempt to gain the information they require from the least intrusive method possible (e.g. checks of existing records, or from reference material), before using more intrusive techniques. As a general rule, the more intrusive the activity, the higher the threshold for authorisation.

Interception of communications

22. Chapter 1 Part 1 of RIPA provides for the interception of communications – that is, the acquisition of the contents of a communication in the course of its transmission. This is the most intrusive form of access. An interception warrant can only be issued by the appropriate Secretary of State if it is both necessary and proportionate in pursuit of a purpose specified on the face of the legislation[2]. RIPA provides for two kinds of interception warrants, both of which must be authorised by a Secretary of State:

- section 8(1) warrants - providing for the interception of communications against a named person or premises; and
- section 8(4) warrants - providing for the interception of external communications and requiring the Secretary of State to certify the extent to which any material obtained can be examined.

23. Additional consideration must be given to whether the degree of intrusion is proportionate if communications relating to religious, medical, journalistic or legal

[2] RIPA provides for interception to be undertaken:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of the UK.

privileged material might be involved; or if dealing with communications which have been collected under a section 8(4) l interception warrant. In some cases, this requires the authorisation of the Secretary of State.

Acquisition of communications data

24. In contrast to the content of data, communications data deals not with *wha*t was said, but rather, when, where and how the communication was made. It is less intrusive but still subject to strong controls. Communications data is held by the communications service provider for their own business purposes and where required to do so under data retention legislation. Public authorities approved by Parliament can only acquire that data under RIPA on a case by case basis, for specified purposes set out in law, and only where it is necessary and proportionate to do so. In addition to this the Agencies may also seek Ministerially authorised interception warrants under RIPA which may additionally authorise the collection of related communications data.

25. Where it is not obtained under a Ministerially authorised warrant, each request for communications data is still subject to a robust internal authorisation process involving an expert guardian and gatekeeper role and the approval of a designated officer. That senior officer must assess the necessity and proportionality of the request, taking into account any collateral intrusion that may occur. Independent oversight of this internal process is provided by the Interception Commissioner and his team of inspectors who examine and test the decision-making of each public authority. This authorisation model was endorsed by the Joint Committee on the Draft Communications Data Bill as being an effective safeguard.

Other information-gathering powers

26. Not all of the material that the Agencies acquire in the course of carrying out their statutory functions is obtained under RIPA. The Agencies may also acquire information/data under their general information powers in section 2(2)(a) of SSA and sections 1, 2(2)(a) and section 4(2)(a) respectively of ISA. In using these powers, they are still public authorities under the Human Rights Act and may only interfere with the right to privacy where it is necessary, proportionate, and for one of the purposes specified in SSA or ISA; and may not acquire data from international partners with the intention of avoiding the need to apply for a warrant under RIPA

27. The Agencies are bound by UK law in their dealings with overseas partners and do not seek to use these relationships to circumvent UK law. When dealing with communications data obtained from overseas partners, for example, GCHQ applies the same standards to its handling of non-RIPA material as it does to RIPA material. This includes a framework of internal controls that ensure that when such material is of greater than usual sensitivity, the necessity and proportionality considerations are subject to review and authorisation by senior staff. In some cases involving the most

sensitive data, even where there is no legal requirement for a Ministerial authorisation, GCHQ may decide that Ministerial approval should be sought.

The compliance culture

28. Alongside the strict legal and policy framework which ensure the activities of the Agencies are authorised and necessary and proportionate, there is also a strong culture and ethos of personal accountability amongst staff in the Agencies. The agencies' recruitment, vetting and training procedures are all designed to ensure that those operating within the ring of secrecy can be trusted to do so lawfully and ethically in accordance with the HRA.

29. More widely, Agency staff report potential inadvertent compliance errors when they see them, so that they can be remedied as quickly as possible and reported to the Commissioners; and they are encouraged to bring any concerns over their work to their management, the central policy team, each Agency's Ethics Counsellor or to the independent Staff Counsellor.

The rigour and reach of independent judicial and parliamentary oversight

30. The Agencies are also subject to rigorous oversight by a number of independent bodies:

(a) **The Commissioners**. These posts are occupied by individuals who hold or have held high judicial office, providing independent scrutiny of the operational activities of the Agencies - including communications data requests, interception warrants, property warrants and surveillance activities – to ensure that their operations are lawful and any intrusion into individuals' privacy is necessary and proportionate.

(b) **The ISC**, made up of senior cross-party parliamentarians. The Committee scrutinises the Government's intelligence activities and reports its findings to Parliament. The Committee's status and statutory oversight remit have been recently enhanced under the Justice and Security Act.

(c) **The IPT** consists of eight senior members of the legal profession and may consider complaints about the use of the RIPA powers by public authorities (including the Agencies) or indeed any 'conduct' by the Agencies. The IPT is the sole appropriate forum for adjudicating on claims against the Agencies alleging infringement of ECHR rights.

31. We are privileged to have some of the finest intelligence and law enforcement agencies in the world. We owe them a tremendous debt. We also owe it to them to ensure that they have the capabilities and powers they need to keep pace with ever changing technology to maintain their ability to tackle terrorism and serious crime. If we are to protect the British public, we need to be a step ahead of the terrorists and the criminals. Our legislation is deliberately designed to be technologically neutral,

but implementation is kept under careful review by the Government to ensure that it allows law enforcement and intelligence agencies to keep pace with rapid changes in the way suspects communicate, while ensuring rigorous safeguards are in place. The advice and recommendations of the Interception Commissioner play an important role in this ongoing process.

Cabinet Office

February 2014