

Statement No 1
For the Respondents
Dated 16 November 2015

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/14/85/CH

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/120-126/CH

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

WITNESS STATEMENT OF CIARAN MARTIN

I, **Ciaran Liam Martin**, of Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

1. I am the Director General for Cyber Security at GCHQ and a member of GCHQ's main Board. In that role, I am responsible for GCHQ's statutory responsibilities for information security in the United Kingdom and its work protecting the UK from cyber threats. I also have wider responsibilities for GCHQ's external communications and policy. I have been in this role since February 2014, having previously served in the Cabinet Office as Director of Constitutional Policy, Director of Security and Intelligence, and head of the Cabinet Secretary's Office. I have been a public official since 1997.

1 of 23

2. I am authorised to make this witness statement on behalf of the Respondents. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within the department.
3. Attached to this statement and marked Exhibit ['CM1'] is a bundle of relevant documents. Tab and page numbers below are references to that Exhibit.
4. In this statement I use the term "the intelligence services" to refer, collectively, to the Security Service, the Secret Intelligence Service and the Government Communications Headquarters. I also use the terms "MI5", "SIS" and "GCHQ" to refer to those bodies individually.
5. In this statement I will (I) address the current intelligence picture and the ongoing challenges posed by changes in technology and developments in the communications market, (II) provide an overview of Computer and Network Exploitation (CNE) and its importance and value in fulfilling GCHQ's statutory functions, before (III) addressing some key safeguards and oversight mechanisms for CNE activities carried out by GCHQ, including:
 - a) The processes for applying for warrants under section 5 of the Intelligence Services Act 1994;
 - b) The processes for applying for section 7 authorisations, including the processes for Secretary of State authorisation and for internal approvals;
 - c) Oversight by the Intelligence Services Commissioner, a retired senior judge;
 - d) Oversight by the Intelligence and Security Committee of Parliament (ISC).

I. THE CURRENT INTELLIGENCE PICTURE

6. The intelligence background to the preliminary issues of law in the *Liberty/Privacy* proceedings was set out in paragraphs 8 to 19 of the witness statement dated 16th May 2014 of Charles Farr, Director General of the Office for Security and Counter Terrorism (OSCT) at the Home Office. I adopt and agree with that statement of the background as it then stood. Given the passage of time, it is necessary to update it and I do so below.
7. Over the past year, the threat to the UK from international terrorism in particular has continued to increase. On the 17 September 2015, Andrew Parker, the Director General of the Security Service (MI5), during an interview with the BBC, revealed that six alleged terror plots targeting the UK have been stopped in the preceding twelve months during an interview with the BBC. In August 2014, the UK threat level, assessed independently by the Joint Terrorism Analysis Centre ("JTAC"), was raised to "SEVERE" from "SUBSTANTIAL", which means that an attack in the UK is highly likely. The principal terrorist threat to the UK continues to derive from militant Islamist terrorists, particularly in Syria and Iraq, where the Islamic State of Iraq and the Levant ("ISIL") has emerged as the most violent of the terrorist groups operating in that region.

8. The recent 2014 Annual Report by the Home Office on the UK's Counter-Terrorism Strategy ("the CONTEST Report"), published on 23 March 2015, highlights the increase in the frequency of terrorist incidents around the world, and the number of fatalities associated with such attacks [CM1-1]. In 2013 (the latest year for which published statistics are available) there were nearly 12,000 terrorist attacks in 91 countries – 40% more than in 2012. These resulted in more than 22,000 fatalities. Just over half of all attacks occurred in three countries: Iraq, Afghanistan and Pakistan. As the Report explains:

"The principal threat continues to come from militant Islamist terrorists, notably in Syria and Iraq. ISIL and other terrorist groups in Syria are now supported by foreign fighters from the UK and other European countries. About 6000 people with extremist connections are among the many Britons who have travelled to the region from the UK. Many have now returned here. Some are likely to have received combat experience and other terrorist related training. Terrorism is being fuelled by an unprecedented quantity of extremist and terrorist propaganda."

9. The murder of two British and other hostages in Syria, apparently by a member of ISIL closely connected to the UK, recent terrible events in Paris and Copenhagen and the 31 Britons killed in the attacks of March and June on a Tunisian museum and beach resort, have underlined the threat posed to British nationals – not just in Syria or Iraq but also outside those arenas, including within the EU. In response to the increase in the UK threat level the Government legislated in 2014 to strengthen the UK's capabilities and provided an uplift in counter-terrorism funding including £130m of additional counter-terrorism funding.

10. The task of defending the UK's interests and protecting its citizens in a digital age is becoming increasingly complicated and challenging and it is one in which GCHQ plays a leading role given its expertise in digital communications technology. The evolution of the internet and modern forms of communications are providing terrorists and criminals with new ways to plan direct and increasingly execute their plots. The CONTEST Report notes that ISIL in particular is using social media "... in an unprecedented quantity and frequency, including personalised messages from UK and other foreign fighters and propaganda from the organisation." As Andrew Parker, the Director General of the Security Service (MI5) explained in a public speech to the Royal United Services Institute (RUSI) on 8 January 2015 [CM1-2]:

"It makes full use of the modern social media and communications methods through which many of us now live our lives. By these means it spreads its message of hate directly in to homes across the United Kingdom – both to those seeking it and those who may be susceptible to its distortion and glamorisation of horrific acts".

11. Robert Hannigan, the Director of GCHQ also drew attention in November 2014 to the way in which ISIL is using the internet to "create a jihadi threat with near-global reach" [CM1-3]. In particular:

"[ISIL] also differs from its predecessors in the security of its communications. This presents an even greater challenge to agencies such as GCHQ. Terrorist have always found ways of hiding their operations. But today mobile technology and smartphones

have increased the options available exponentially. Techniques for encrypting messages or making them anonymous which were once the preserve of the most sophisticated criminals or nation states now come as standard. These are supplemented by freely available programs and apps adding extra layers of security, many of them proudly advertising that they are “Snowden approved”. There is no doubt that young foreign fighters have learnt and benefited from the leaks of the past two years.”

12. The diversification of the communications market and the ability of terrorists, criminals and others to exploit new internet-based technologies has made it increasingly difficult for GCHQ and the other intelligence services to monitor the communications of those who present a threat to UK interests. Unless the intelligence services are able to maintain their capabilities in the face of these unprecedented technological challenges, the UK will be unable to obtain the intelligence it needs to counter these threats. As the Chief of SIS made clear in his speech to English Heritage in March 2015, the intelligence services are engaged “... in a technology arms race” [CM1-4].

13. Mr Parker, the Head of MI5, discussed the changing nature of the challenges that the intelligence services face in his BBC interview of 17 September 2015 [CM1-6]:

“We need to be able to use data sets so we can join the dots, to be able to find and stop the terrorists who mean us harm before they are able to bring the plots to fruition. We have been pretty successful at that in recent years but it is becoming more difficult to do that as technology changes faster and faster.”

14. The threat to the UK does not stem just from terrorism. For example, as David Anderson QC noted in his independent report on investigatory powers, *A Question of Trust*, [CM1-7], GCHQ used analysis of bulk data to track down two men overseas who had been harnessing the vulnerabilities of the web to blackmail hundreds of children across the world, including the UK, into exposing themselves online – causing them huge trauma. Some of the victims self-harmed and considered suicide. It was the vital work of GCHQ analysts that brought this abuse to an end: they were able to confirm the suspects’ names and locations, and to identify an accomplice. After liaison between law enforcement agencies, the two men were arrested and jailed in their home country.

15. But this work tackling national security threats in the digital age is getting harder. One important challenge is the implication of the use of encrypted communications. Encryption is important for computer security and GCHQ advocates its use in the UK as part of good cyber security practice. But the rise of encryption offered by telecommunications companies to their customers has impacted particularly severely on GCHQ’s intelligence capabilities because encrypted data acquired lawfully by GCHQ may be unreadable to the intelligence services. The challenges posed by the growth of encryption have become particularly acute over the course of the last two years as telecommunications companies increasingly use improved privacy protections, including encryption by default, as part of their marketing strategies. According to the Director of Europol encryption has now become [CM1-8]:

“... the biggest problem for the police and the security service authorities in dealing with the threats from terrorism... It’s changed the very nature of counter-terrorist work from

one that has been traditionally reliant on having good monitoring capability of communications to one that essentially doesn't provide that anymore."

16. The US authorities have experienced similar problems relating to the growth of encryption which they refer to as "Going Dark". The Director of the FBI recently explained [CM1-9]:

"Encryption just isn't a technical feature, it's part of a marketing pitch, but it will have very serious consequences for law enforcement and national security agencies at all levels... There should be no law-free zones in this country..."

17. In a public speech given to RUSI on 10 March 2015, the Foreign Secretary offered a summary of the challenges posed by the accelerating pace of technological change [CM1-10]:

"And as the range of threats gets bigger, so the pace of technological change with which the Agencies must keep pace is getting faster, making their central task of keeping us safe ever more demanding. The Agencies have always had to innovate to stay one step ahead of their adversaries. But the accelerating pace of technological change has upped the ante as terrorists, states and others who would do us harm embrace, adapt, and abuse the technology that we so readily welcome in our everyday lives.

And it is a truism that as technology enables greater productivity, it also open us up to greater vulnerability. So our Agencies must master every technological advance. They must understand its strengths, its weaknesses, the vulnerabilities it introduces – before our enemies can turn it against us".

18. The Security and Intelligence Agencies Financial Statement of June 2014 recognises that the need to maintain capabilities in the face of these rapid technological changes is perhaps the greatest challenge currently faced by the intelligence services [CM1-11].

19. David Anderson QC also highlighted the impact of these challenges in his annual report of the Terrorism Acts (September 2015) [CM1-12]:

"It has been a feature of several major terrorist attacks, including the 7/7 bombings, the killing of Lee Rigby and the French shootings in January 2015, that one or more of the perpetrators was known to the police or security services but had not been assessed as posing a major risk at the time. The speed with which things can change, and the difficulties in knowing how best to prioritise limited surveillance resources, were illustrated in unprecedented detail by the inquiry of Parliament's Intelligence and Security Committee into Lee Rigby's killing."

20. The age of ubiquitous encryption means, inter alia, that GCHQ and the other intelligence agencies require a more innovative and agile set of technical capabilities to meet the serious national security challenges of the digital age. Computer and Network Exploitation (CNE) is one such capability. CNE operations have been authorised by senior Ministers for many years since the 1994 Act, but its importance relative to GCHQ's overall capabilities has been increasing significantly in recent years and is likely to increase further. The allegations made in both claims concern activities known by the

intelligence services as CNE, so it is necessary to describe in more detail what CNE operations are.

II. AN OVERVIEW OF CNE AND ITS IMPORTANCE AND VALUE

Computer and Network Exploitation (“CNE”)

21. CNE is a set of techniques through which an individual gains covert and remote access to a computer (including both networked and mobile computer devices) typically with a view to obtaining information from it. GCHQ carries out CNE operations as part of its intelligence-gathering activities, as set out below.
22. CNE operations vary in complexity. A straightforward example is the use of the login credentials of a target to gain access to the data held on a computer. The login credentials could belong to a normal user or an entity with elevated privileges such as an administrator.
23. More sophisticated CNE operations involve taking advantage of weaknesses in software. For instance a piece of software may have a “vulnerability”: a shortcoming in the coding that may permit the development of an “exploit”, typically a piece of software, a chunk of data, or a sequence of commands that takes advantage of the vulnerability in order to cause unintended or unanticipated behaviour to occur. This unanticipated behaviour might include allowing another piece of software – an implant, sometimes called a “backdoor” or a “Trojan” - to be installed on the device.
24. The exploit and subsequent implant can be delivered in a number of ways. Two of the techniques are:
 - a) The user of a device might be sent an e-mail inviting them to open a link or document of interest. When the user clicks on the link or document, it takes them to website that delivers the implant. This is known as “phishing”.
 - b) Alternatively, an individual with access to a computer might insert the implant using, for example, a USB stick, whether wittingly or otherwise.
25. The function of an implant may also vary in complexity. A simple implant will typically explore the target computer, sending back information over the internet to its controller. Others might monitor the activity of the user of the target device, or take control of the computer.
26. As with interception, there are a range of circumstances in which a state may require its intelligence services to conduct this type of activity. CNE can be a critical tool in investigations into the full range of threats to the UK from terrorism, serious and organised crime and other national security threats. For example, CNE enables the state to obtain the valuable intelligence it needs to protect its citizens from individuals engaged in terrorist attack planning, kidnapping, espionage or serious organised criminality.

27. CNE operations may enable GCHQ to obtain communications and data of individuals who are engaged in activities that are criminal or harmful to national security. Such circumstances may arise where, for example:
- a) the fact that the wanted communications were not in the course of their transmission and could not therefore be intercepted;
 - b) the absence of any Communications Services Providers (CSPs) on whom a warrant can be served to acquire particular communications; and
 - c) the greater possibility of acquiring a comprehensive set of the target's communications/data by means of CNE.

Importance and value of CNE

28. As discussed above, CNE is a critical tool in the investigation of threats to the UK. The UK Government does not have the same ability to identify individuals and entities outside the UK who may pose a threat to national security as compared with those within the UK. Outside the UK, GCHQ's capabilities are the key sovereign intelligence-gathering capabilities available to the Government.
29. Historically, GCHQ's ability to identify individuals of intelligence interest has been based largely on bulk interception. This capability remains critical to the identification and mitigation of threats, but increasingly it is being threatened by the unprecedented technological challenges outlined in part (I) of my statement. As the Foreign Secretary explained in his speech to RUSI:
- “...And to GCHQ, although since its birth a signals intelligence organisation, the rapid pace of the development of the internet and the sheer scale of its traffic, pose new challenges – finding the needle of vital information to safeguard our security in a hay stack that is growing exponentially and is already well beyond the capacity of human analysis.”
30. As noted in the previous section, the introduction of strong encryption across many web services in the wake of the Snowden allegations has posed particular technological challenges. The spread of encryption has impeded intelligence service access to communications. In his own speech to RUSI on “terrorism, technology and accountability, Andrew Parker, the Director General of MI5 said:
- “Changes in the technology that people are using to communicate are making it harder for the Agencies to maintain the capability to intercept the communications of terrorists. Wherever we lose visibility of what they are saying to each other, so our ability to understand and mitigate the threat that they pose is reduced.”
31. In the light of these developments, CNE is increasingly required to enable GCHQ to continue to obtain the intelligence the Government requires to identify individuals outside the UK who may pose a threat to national security. Indeed CNE may in some cases be the only way to acquire intelligence coverage of a terrorist suspect or serious

criminal in a foreign country. As noted by the Intelligence and Security Committee at page 67 of its Privacy and Security Report [CM1-13]:

“During 2013 a significant number of GCHQ’s intelligence reports contained information that derived from IT operations against a target’s computer or network.....”

32. At the same time as GCHQ is adapting to meet these new technological challenges, there is an increasing expectation within Government that GCHQ will play a lead role in improving cyber security for the protection of the UK’s vital national interest in an era where threats to the UK from cyber space are growing very rapidly. GCHQ plays a key role in securing the safety of the internet for the benefit of the public as I explain further below. CNE is an important part of GCHQ’s ability to understand, detect and disrupt cyber threats to the UK.
33. GCHQ’s CNE capabilities have made a vital contribution to counter the increased threat to the UK from militant Islamist terrorists. And, as noted in the previous section, GCHQ’s CNE capabilities have also enabled the disruption of paedophile-related crime. I cannot say more about these operations in this open, public statement without undermining the interests of national security and the prevention and detection of serious crime.
34. CNE has long been an essential part of GCHQ’s capabilities. It has become increasingly important in recent years and will become more important yet in the years ahead. Without it, GCHQ’s ability to protect the public from terrorism, cyber attack, serious crime, including child sexual exploitation, and a range of other threats would be seriously degraded.

The Claimant’s allegations about CNE

35. The Claimants make a number of general and specific allegations in the two Claims. Before addressing the specific allegations made by the Complainants, I would like to make four preliminary points in relation to the general allegations.
36. First, the Claimants allege that the tools used by GCHQ allow huge amounts of information (current and historical) to be extracted from “millions” of devices thereby subjecting users to mass and intrusive surveillance. Allegations that GCHQ conducts “mass surveillance” were made by one of the Claimants in the context of a previous complaint before this Tribunal. On that occasion the Tribunal stated “we are entirely clear that the Respondents are not seeking, nor asserting that the system entitles them to seek, to carry out what has been described as “*mass*” or “*bulk*” surveillance”. I should like to make clear that it is equally the case that GCHQ neither seeks, nor believes that we are entitled to seek to carry out indiscriminate mass surveillance activities of the sort alleged in this case. They are also precluded by the clear statutory framework which regulates GCHQ’s activities. CNE must be authorised by a Secretary of State and is subject to strict tests of necessity, proportionality and legitimate aim as set out in the Intelligence Services Act 1994. These authorisations, and the internal processes that GCHQ has in place to manage the authorised activities, are subject to independent scrutiny by the Intelligence Services Commissioner. In February 2015, the Government published a draft Equipment Interference Code of Practice. It set out the strong

safeguards that GCHQ has always applied to CNE activities. More generally, any conduct by GCHQ must be consistent with its statutory functions and the purposes for which those functions may be exercised. As the ISC has recently made clear in its report on Privacy and Security:

“We are satisfied that the UK’s intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do.”

37. It follows that a significant proportion of the examples given in the Claimants’ evidence with respect to the possibilities created by CNE tools bear no relation to the reality of GCHQ’s activity and/or would be unlawful having regard to the relevant statutory regime.
38. Secondly, the Claimants allege that CNE may create potential security vulnerabilities or leave users vulnerable to further damage.
39. Intelligence work by its nature is secret – both the how and the specific targets. It is therefore in GCHQ’s interests to carry out CNE operations in such a way that the activity is not apparent to the target, nor to others wanting to know who the specific targets of HMG intelligence activities are. GCHQ does not intrude into privacy any more than is necessary to discharge our functions. Nor would it be right to enable others to intrude into privacy. To leave targets open to exploitation by others would increase the risk that their privacy would be unnecessarily intruded upon. It would also increase the risk of those who wish to know who our targets are identifying GCHQ’s tools and techniques. Operations are therefore carried out in such a way as to minimise that risk.
40. I should also like to take this opportunity to explain GCHQ’s role more generally in securing the safety of the internet for the benefit of the public. The internet is an intrinsically insecure environment, with billions of computers constantly running millions of complex programmes. PwC’s 2015 Information security breaches survey [CM1-5] reported that 90% of large organisations and 74% of small businesses had a security breach in the period covered by the report; the average cost of the worst serious breach ranged from £1.46m to £3.14m for large organisations; £75,000 to £311,000 for small businesses. GCHQ’s role is to play its part in helping to make the internet as safe as possible for ordinary citizens and legitimate businesses, and prevent its use by criminals and terrorists. We engage with strategically important organisations who are particularly vulnerable to cyber attack, and we also promote high standards of cyber security across all sectors of the UK, including by recommending the use of strong encryption.
41. One element of GCHQ’s information assurance work concerns the finding and reporting of vulnerabilities in digital technologies. GCHQ helps technology providers identify weaknesses in finished hardware and software; we also help uncover potential issues at the design stage, often before they become major in-service problems – saving firms time and money. Some but not all vendors choose to publicly credit GCHQ for finding those weaknesses. For example, in September of this year, Apple publicly credited CESG, the Information Security arm of GCHQ, with the detection of a vulnerability in their iOS operating system which could have been exploited to allow the unauthorised modification of software on devices such as iPhones and iPads, the extraction of information from

those devices, or to disrupt their operation. That vulnerability has now been patched. In the last two years, GCHQ has disclosed vulnerabilities in every major mobile and desktop platform, including the big names that underpin British business.

42. Thirdly, while CNE operations can be highly intrusive, they are not in general any more intrusive than any other operations conducted by GCHQ under the Regulation of Investigatory Powers Act 2000 (“RIPA”) or the Intelligence Services Act 1994 (“ISA”).
43. By way of example, Part II of RIPA permits certain public authorities to authorise intrusive surveillance in relation to residential premises and private vehicles. A listening device located within a private address - potentially including a bedroom – clearly has the potential to obtain private information relating to all the occupants of that address (including non-targets) of an extremely sensitive and personal nature. Information of this nature which is communicated between two or more people within a residential address or a private vehicle may well contain content that those individuals would deem too personal, private or sensitive to commit to writing and store on a device. Nonetheless, such highly intrusive surveillance is lawful if properly authorised, having met the tests of necessity and proportionality.
44. Similarly, while CNE operations can be used to access a wide range of data, they are not in general any more intrusive than the interception of communications under Chapter I of Part I of RIPA. With the advent of Cloud storage (which many people opt to use), all the material referred to by the Claimants in their complaints would be potentially available to the intercepting agencies via interception – including photographs, videos, passwords, banking details, passport details, etc. All of this material could, in principle, be acquired by way of interception.
45. In summary, while the level of intrusiveness will clearly vary depending on the type of activity in issue, I do not therefore believe it is the case that GCHQ’s CNE operations are in general any more intrusive than its other operations involving interception, surveillance or other investigative techniques.
46. Fourthly and finally, GCHQ recognises that CNE activity could theoretically change the material on a computer. For example the installation of an implant would itself amount to a change. However it would be neither necessary nor proportionate, nor would it be operationally sensible, for an organisation seeking to use CNE for intelligence gathering purposes to make more than the most minimal, and to the greatest extent possible, transient, changes to targeted devices.

III. SAFEGUARDS AND OVERSIGHT MECHANISMS

Overview

47. The regime governing GCHQ’s CNE activities consists of provisions in primary legislation and in relevant Codes of Practice and also in relevant internal arrangements and safeguards which are applied by GCHQ.

48. I explain below the key components of the application process for CNE warrants and authorisations, and the oversight arrangements governing GCHQ's CNE activities. These processes are supplemented by the Equipment Interference Code of Practice [CMI-14] which contains important safeguards including:
- a) Detailed guidance on the requirement of proportionality and the considerations which apply in the CNE context, including issues such as collateral intrusion and the need to consider less intrusive alternatives (Chapter 2);
 - b) Guidance on the frequency of reviews, particularly where there is a high level of intrusion into private life or significant collateral intrusion or confidential information is likely to be obtained (Chapter 2 at §§2.13-2.15);
 - c) Best practice guidance on applications for warrants/authorisations (§§2.16-2.17);
 - d) Special considerations which should apply to legally privileged and confidential information (Chapter 3);
 - e) Detailed and comprehensive procedures for the authorisation of both sections 5 and 7 ISA equipment interference activity (see Chapters 4 and 7);
 - f) Important record keeping requirements in respect of any CNE (Chapter 5);
 - g) Comprehensive safeguards and guidance as regards the processing, retention, disclosure, deletion and destruction of any information obtained by the intelligence services pursuant to interference CNE warrant, which mirror similar safeguards applied as part of the interception regime pursuant to section 15 of RIPA (Chapter 6).
49. GCHQ's internal arrangements are safeguards set out in the Respondents' Closed Response and Closed witness evidence. I also refer to certain of the internal arrangements in this statement. They include the Compliance Guide, which is a document which is made available electronically to all GCHQ staff. It comprises mandatory policies and practices which apply to all GCHQ operational activity and has been approved by the Foreign Secretary and the Interception of Communications Commissioner. The electronic version of the Compliance Guide was made available to staff in late 2008 and there have been no substantive changes since then, although it has been amended in minor ways to ensure that it remains up to date. The Compliance Guide requires all GCHQ operational activity, including CNE activity, to be carried out in accordance with three core principles. These are that all operational activity be:
- a) Authorised (generally through a warrant or equivalent legal authorisation);
 - b) Necessary for one of GCHQ's operational purposes; and
 - c) Proportionate.
- 49A. These principles and their application to specific activities conducted by GCHQ, are referred to throughout the Compliance Guide. They are also specifically referred to in the additional CNE-specific internal guidance referred to below. In short, they are core requirements which run through all the guidance which applies to GCHQ's operational activities, including CNE.
- 49B. In addition, pursuant to GCHQ's Compliance Guide and Intelligence Sharing and Release Policy (a policy document governing the sharing and release of operational data), the position is that all operational warrant is handled, disclosed and shared as

though it had been intercepted under a RIPA warrant. The term “operational material” extends to all information obtained via CNE, as well as material obtained as a result of interception under RIPA.

- 49C. GCHQ’s internal arrangements also address the role of the Reporting Quality Checker in ensuring that any release of intelligence outside of GCHQ is lawful and proportionate.
- 49D. GCHQ has a collaborative relationship with the NSA. Activities forming part of that relationship must be undertaken in accordance with the principles set out in the Compliance Guide, which emphasises the need for all operational activity to be necessary and proportionate.

Authorising CNE: section 5 and 7 ISA

50. GCHQ conducts all CNE activity pursuant to warrants under section 5 of the ISA or authorisations under section 7 of the ISA. I have set out below an explanation of the differences between the section 5 ISA regime and the section 7 ISA regime as it applies to GCHQ’s activities. I have also identified the detailed safeguards which regulate this activity including:

- a) The processes for applying for, renewing and cancelling section 5 warrants;
- b) The processes for gaining section 7 authorisations, including the processes for Secretary of State authorisation and for internal approvals;
- c) Oversight by the Intelligence Services Commissioner;
- d) Oversight by the Intelligence and Security Committee of Parliament (ISC).

51. These safeguards and oversight mechanisms are reflected in the Covert Surveillance and Property Interference Code and the draft Equipment Interference Code of Practice

a) The processes for applying for section 5 warrants

52. The section 5 ISA regime is used primarily by GCHQ to authorise CNE operations against specific equipment located within the UK. Section 5(2) of ISA provides that the Secretary of State may, on an application made by GCHQ, issue a warrant authorising the taking of action in respect of property as specified in that warrant if he: thinks it necessary for the action to be taken for the purpose of GCHQ in carrying out any function that falls within section 3(1)(a) of ISA; is satisfied that the taking of action is proportionate to what the action seeks to achieve; and is satisfied that satisfactory arrangements are in force under section 4(2)(a) of ISA with respect to the disclosure of information obtained by virtue of this section and that any information obtained under the warrant will be subject to those arrangements.

53. Applications for section 5 warrants in respect of CNE must contain all the detailed matters as set out in paragraph 4.6 of the current draft Equipment Interference Code of Practice. Prior to the publication of this draft Code of Practice on 5 February 2015 applications were required to conform with paragraph 7.37 of the Covert Surveillance and Property Interference Revised Code of Practice published on 10 December 2014 [CM1-15]. This required GCHQ to provide the same information in support of an application as

would be required when the police, the services police, National Crime Agency (NCA), HM Revenue and Customs (HMRC) or Competition and Markets Authority (CMA) were making an application to an authorising officer. The details of this information are set out in paragraph 7.18 of the Surveillance and Property Interference Revised Code of Practice. These requirements (and the numbers of the relevant paragraphs) were unchanged from previous versions of the Code of Practice published in [2000] and revised in 2010.

- 53A. The section of the Compliance Guide which specifically concerns CNE states that authorisation is required under the ISA in order to address the liability which most CNE operations would normally attract under the Computer Misuse Act 1990. The requirement for a section 5 warrant for CNE operations on computers in the UK is made clear. Section 5 warrants are also addressed in the Compliance Guide as follows:

“A Secretary of State must approve a new ISA s.5 warrant. Renewal is required after six months. In an emergency, a new temporary warrant may be issued by a GCHQ official of appropriate seniority if a Secretary of State has expressly authorised its use.”

- 53B. GCHQ also has separate specific internal guidance governing applying for, renewing and cancelling section 5 warrants (“the Section 5 Guidance”). This was updated in January 2015. The internal guidance is regularly reviewed to ensure that it remains comprehensive and pertinent as GCHQ’s CNE activities continue to evolve. The Section 5 Guidance, application forms and warrant templates were updated following a visit of the Intelligence Services Commissioner (Sir Mark Waller) in June 2013. During that visit the Intelligence Services Commissioner acknowledged that GCHQ gave due consideration to privacy issues, but commented that he would like to see greater evidence of this reflected in warrants and submissions, in particular in relation to why the likely level of intrusion, both into the target’s privacy and the collateral intrusion into the privacy of others, was outweighed by the intelligence to be gained. In response, GCHQ updated its s.5 (as well as its s.7) application forms, warrant templates and guidance to advise staff on the type and level of detail required. At his next inspection in December 2013, the Intelligence Services Commissioner was provided with these documents and stated that he was content with the actions that had been taken.

b) The processes for applying for section 7 authorisations, including the processes for Secretary of State authorisation and for internal approvals

The importance of CNE as an overseas intelligence gathering capability

54. As I have already explained, the UK Government does not have the same ability to identify individuals outside the UK who may pose a threat to national security as compared with those within the UK. Outside the UK, GCHQ’s capabilities are the key sovereign intelligence-gathering capabilities available to the Government.
55. There are important practical differences between gathering intelligence on individuals, organisations and equipment within the UK and gathering intelligence on individuals, organisations and equipment that exist or operate outside that jurisdiction. These

practical differences are reflected in the authorisation regimes provided by sections 5 and 7 of the ISA.

56. As mentioned above, the section 5 ISA regime is used primarily by GCHQ to authorise CNE operations against specific equipment located within the UK. By contrast, section 7 permits the giving of class authorisations which do not require the authorisation to name or describe a particular piece of equipment, or an individual user of the equipment. Consequently CNE is authorised in relation to equipment located outside the UK pursuant to a section 7 class authorisation and internal approvals. This reflects practical realities of intelligence gathering outside the UK, where GCHQ requires the flexibility to obtain material which will contain intelligence relevant to the safeguarding of the UK's national security without knowing in advance from which particular piece of equipment that material may be obtained.
57. In line with the foregoing, a class authorisation under section 7 ISA is sought wherever members of GCHQ conduct CNE in relation to equipment located outside the UK that would otherwise be unlawful. This includes cases where the act is done in the UK, but is intended to be done in relation to apparatus that is or is believed to be outside the UK, or in relation to anything appearing to originate from such apparatus. In addition GCHQ will obtain a section 7 authorisation for any CNE activities carried out abroad or over a foreign computer, even if the relevant user is located in the UK. Paragraph 7.4 of the current draft Equipment Interference Code of Practice sets out the additional safeguards which apply if either the subject of a section 7 operation is known to be in the UK, or the equipment is brought to the UK during the currency of the authorisation.
58. While GCHQ's section 7 CNE class authorisation offers the potential for broader and more flexible acquisition of intelligence than is permitted under its section 5 warrants, the process described below for giving section 7 authorisations, in combination with GCHQ's system of internal approvals and additions, ensures that its activities are properly regulated and subject to strict safeguards and oversight.

Section 7 authorisations

59. Section 7 ISA provides that an authorisation has to be issued personally by the Secretary of State on an application to him to that effect. The purposes for which warrants are issued are set out in section 7(3) ISA.
60. Section 7(1) of ISA provides that a person shall not be liable in the United Kingdom for any act done outside the UK for which he would be liable, if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under that section.
61. Paragraph 7.1 of the current draft Equipment Interference Code of Practice requires that GCHQ applies the provisions of that Code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of ISA. Paragraph 7.7 of the current draft Equipment Interference Code of Practice states that an application for the giving or renewal of a section 7 authorisation should contain the same information, as far as is reasonably practicable in the circumstances, as an application for a section 5 CNE warrant.

62. Paragraph 7.11 of the current draft Equipment Interference Code of Practice states that an authorisation under section 7 may relate to a broad class of operations. Paragraph 7.12 states that where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of CNE must be sought from a designated senior official. In any case where the CNE activity may result in the acquisition of confidential information, authorisation must be sought from an Annex A approving officer (and in the case of GCHQ an Annex A approving Officer is someone in a small group of GCHQ's most senior managers).
63. Applications for section 7 authorisations must, as far as is reasonably practicable in the circumstances, contain all the detailed matters set out in paragraph [4.6] of the EI Code. The process by which GCHQ obtains Secretary of State authorisation for class authorisations under section 7 of the ISA has evolved over the last few years with an increasing emphasis on providing detailed information to the Secretary of State about the type of CNE activities covered by the class authorisation. Since July 2014 GCHQ has copied to the FCO all of its internal section 7 approvals for CNE operations which were given pursuant to the class authorisation. In August 2013 GCHQ recommended that, in future, the internal approvals should be sent through the relevant department in the FCO to the Secretary of State and this was agreed by the FCO.

Internal approvals

64. Where a class authorisation has been given by the Secretary of State under section 7, internal Approval to conduct individual operations under that authorisation in respect of CNE must also be sought from a designated senior official.
65. Before granting an approval, the senior official must be satisfied that the proposed operations are necessary, proportionate and within the scope of the class authorisation. Approval may only be given where operations are necessary in the interests of national security, for the prevention and detection of serious crime or in the interests of the economic wellbeing of the UK. In addition, the senior official must be satisfied that the nature and degree of the proposed intrusion against target computers is proportionate and limited to that required for the operation to be effective, and that safeguards are in place to ensure that any aspect of the operation or the data thus obtained is handled in a manner consistent with GCHQ's legal obligations under Intelligence Services Act and the Human Rights Act. Feeding into the internal approvals process is an internal specialist risk assessment panel, involving a range of relevant technical, operational and policy leads. This panel provides expert oversight and assurance to operators, policy leads and senior leadership that the tools and techniques being used, and the way in which they are being used, present an acceptable level of technical and operational risk. Key agreements and decisions made by the internal specialist risk assessment panel are documented. They provide an audit trail and a 'history' of decisions (which, for example, are used to inform risk assessment statements made in section 7 approval requests and political submissions).
66. GCHQ copies to the Foreign and Commonwealth Office all of its internal s.7 approvals and extensions for CNE implant operations which were given pursuant to the class

authorisation. In addition, if an operation is judged to present significant risk, the proposal will be submitted to FCO officials or the Secretary of State (and GCHQ will also seek FCO legal advice if a proposed operation involves issues of international law).

66A. The Section 7 Guidance also deals with the situation where there is a significant change to an existing approval, or when a new target is proposed with the result that an “addition” to an existing approval is required.

Additions

67. Under an internal approval, operations against specific targets are authorised by means of an ‘addition’. The term “addition” is not specifically defined in GCHQ’s internal arrangements, but is used within GCHQ to refer to the process and associated formal documentation for the inclusion of further specific targets within the scope of an existing internal approval for a CNE operation. The “additions form” requires the same regard to be had to justification, necessity and proportionality as is required for an initial approval.

68. The level of detail in an addition will be tailored to the operation in question, but it will describe the specific target (which must fit within the description of the target set in the relevant internal approval) and the necessity and proportionality of the planned operation, as well as how intrusion into privacy will be managed. The addition will also describe the planned activity and assess the risks associated with this (which must fit within the thresholds set in the relevant internal approval). The role and seniority of the authoriser for additions depends on factors including the sensitivity and complexity of the planned activity, but the authoriser must always have been trained before assuming the role.

68A. Analysts will have assigned to them a point of contact within the CNE operational team with whom they can speak about operational matters. In addition, within their own team they will have a dedicated point of contact with whom they can discuss any legal and policy questions.

Records

68B. GCHQ creates and maintains records of the application for, renewal of, approval of and cancellation of all warrants under section 5 and class authorisations and internal approvals under section 7 indefinitely. These include any comments or stipulations from the Secretary of State relating to them.

Training

68C. GCHQ has a comprehensive programme of training and testing in place for those involved in CNE operations and for intelligence analysts who may have access to data obtained in CNE operations. This training includes operational and mandatory legalities training. The training involves testing and regular reassessment.

c) Oversight by the Intelligence Services Commissioner

The Commissioner

69. GCHQ's CNE operations are overseen by the Intelligence Services Commissioner under section 59(1) of RIPA. The Rt Hon Sir Mark Waller currently holds this role and he was appointed by the Prime Minister on 1 January 2011. His predecessor was Sir Peter Gibson (also a former Lord Justice of Appeal).
70. The functions of the Intelligence Services Commissioner, as they relate to CNE, are:
- a) To keep under review the exercise by the Secretary of State of his powers to issue, renew and cancel warrants under sections 5 and 6 of ISA;
 - b) To keep under review the exercise by the Secretary of State of his powers to give, renew, and cancel authorisations under section 7 of ISA;
 - c) To give the Tribunal all such assistance (including my opinion on any issue falling to be determined by it) as it may require in connection with its investigation, consideration or determination of any matter;
 - d) To make an annual report to the Prime Minister on the carrying out of my functions, such report to be laid before Parliament.
71. The Intelligence Services Commissioner formally inspects GCHQ's CNE activity twice a year, and also makes ad hoc visits to look at particular aspects of its work in more depth. These are known as 'under the bonnet' visits. During the formal inspections the Commissioner raises inquiries, examines procedures and examines the relevant paperwork for a selection of warrants, class authorisations (including internal approvals and relevant additions), that he personally has chosen in advance, to ensure that it is in order and that, in particular, sufficient consideration has been given to issues like collateral intrusion and privacy. In order to permit the Commissioner to make a selection of the documents he wishes to see, GCHQ provides him with a "choice letter" containing:
- a) Summaries of all section 5 ISA warrants and section 7 ISA class authorisations that are either in place or which have been cancelled or allowed to expire since the previous choice letter, including all internal approvals underneath the latter. Those warrants and class authorisations that the Commissioner has previously inspected are flagged as such;
 - b) A list of errors reported to the Commissioner since the previous Review;
 - c) A list of intelligence reports at least partially sourced from CNE operations, which contain confidential or legally privileged material issued since the previous choice letter;
 - d) A list of all warrants and authorisations examined at previous reviews by the current Commissioner.
- 71A. As part of the **September 2010** visit, Sir Peter Gibson discussed a recently reported CNE error which led to a change being made in warrant applications.
- 71B. During Sir Mark Waller's visit in **March 2011** he commented on the section 7 approvals and noted that 'proportionality' appeared in its own right on the section 7 approval form, but would have liked to see 'necessity' appear in its own right on the form. This change was subsequently introduced.

- 71C. During the **December 2013** Inspection the Commissioner expressed himself content with the actions GCHQ had taken in respect of documenting privacy considerations in warrant and authorisation application paperwork since June 2013.
- 71D. Following the discovery of a typographical error relating to the expiry date of the renewal of a section 5 warrant the Commissioner had asked that the Secretary of State amend the face of the instrument in his own hand and initial the change. The Commissioner queried why the error had not been picked up sooner and asked to see a copy of the checklist that is used to check warrants before they go up to FCO. He asked that the list be supplemented with a further check to be carried out when the signed warrant is returned from the warrant issuing department to ensure that any future mistakes are picked up at an early stage. He also asked to be informed if there were any similar instances in the future and this was agreed.
- 71E. There was also a discussion of what information should be included on warrant renewal instruments. It was explained that, until recent years, renewal instruments for section 5 warrants had contained the minimum wording stipulated by ISA section 6. GCHQ had subsequently added a description of the property (which made it easier to see to what a renewal instrument referred), and, prompted by the Commissioner, had then added a final paragraph reminding the Secretary of State of his statutory obligations when signing the renewal. The Commissioner's view was sought as to whether it would be helpful to add a description of the actions authorised by the warrant. Sir Mark felt that, if we were minded to make further changes to the renewal instrument, we might consider including all the relevant wording from the original instrument.
- 71F. In **the May 2014** Inspection the Commissioner recommended a new form of words for section 5 warrants which make clear that the Secretary of State is authorising on the basis that GCHQ will act in accordance with the accompanying submission. He also made recommendations about the conditions set out in the submissions and instruments. He continued to monitor thematic property warrants closely.
- 71G. In the **November 2014** Inspection the Commissioner expressed himself content that GCHQ record on the warrant instrument that we will comply with any conditions set out in the accompanying submission as this formally joins the warrant to the submission.
- 71H. There was also discussion about section 5 ISA warrants that are "thematic" rather than relating to specific property. The Commissioner asked that section 5 warrants should relate to specific property wherever possible rather than relying on a thematic warrant. Overall the Commissioner indicated that he was content for such warrants to be used, where there is no intrusion into privacy, but emphasised that they should be the exception and not the rule.
- 71I. The Commissioner's **April 2015** Inspection was the first inspection at which the Commissioner formally inspected the Additions layer (under internal approvals) for the s.7 authorisations process. As already set out above, this is the layer at which individual targets are usually described. The Commissioner recommended changes be

made to ensure that each element is dealt with explicitly and at the earliest opportunity. These changes have been implemented.

- 71J. Sir Mark Waller has conducted a number of what he refers to as “under the bonnet” visits, separate from his formal inspections.
- a) On 20 January 2012 Sir Mark was briefed on GCHQ’s CNE activities.
 - b) On 10 July 2013 Sir Mark sat in on one of the legalities courses.
 - c) On 11 September 2014 Sir Mark visited GCHQ following an approach to him by a BBC journalist, following media reports about certain alleged CNE activities.
- 71K. The Commissioner’s most recent “under the bonnet” visit was on 9 December 2014. This visit was intended to give him an overview of GCHQ’s operational use of CNE so that he could see how our internal governance processes meshed with the authorisation regime. During the visit we established that Sir Mark fully understood the section 5 authorisation regime, so the focus was primarily on operational activity authorised under ISA s.7, and how GCHQ used its internal hierarchy of approvals and additions. Sir Mark was briefed on the internal approvals process, and the circumstances where GCHQ would seek political approval for activities.
- 71L. I am aware that the Intelligence and Security Committee of Parliament, in their report of 12 March 2015, “Privacy and Security: A modern and transparent legal framework”, addressed section 7 authorised operations at paragraphs 177ff and said this at Recommendation BB on page 66:

“While intrusive action within the UK requires a Ministerial warrant, outside the UK it is authorised by the use of a Class Authorisation under the Intelligence Services Act 1994. However, the Agencies do not all keep detailed records of operational activity conducted under these Class Authorisations. It is essential that they keep comprehensive and accurate records of when they use these powers. It is unacceptable not to record information on intrusive action.”

Given the Commissioner’s clear endorsement of GCHQ’s internal section 7 processes and the associated record keeping undertaken by GCHQ (the “audit trail” in the Commissioner’s words), I do not consider that this statement relates to GCHQ’s CNE operations. As set out earlier in this statement GCHQ does keep very detailed records of CNE activity conducted pursuant to section 7 authorisations, including all details of internal Approvals and Additions.

- 71M. Finally, it is to be noted that we have an established process for reporting errors to the Commissioner. In particular error reports follow a standard structure with sections addressing:
- o The background;
 - o How and why was it identified?
 - o What was the magnitude of the error?
 - o Why did this happen?
 - o How we’ll make sure it never happens again.

Reports of the Commissioner

72. In his formal reports, the Commissioner has explained the extent of his oversight of GCHQ's CNE activities and made a number of positive comments about GCHQ's CNE operations and the thoroughness of its processes. In his report for 2013 [CM1-20] the commissioner stated:

"From my work it is clear to me that GCHQ apply the same human rights considerations and the same privacy considerations, checks and balances to the virtual world as they do to the real world. From my scrutiny of GCHQ authorisations, inspection visits and my under the bonnet work, it is my view that GCHQ staff continue to conduct themselves with the highest level of integrity and legal compliance."

72A. In his Report for 2014 [CM1-16] the Commissioner explained the nature of his review functions and highlighted the extent of co-operation which he received from the Agencies in this regard. He stated:

"I emphasise that I do this activity personally and I undertake my duty rigorously and entirely independently of government, Parliament and the intelligence agencies themselves, without political favour or personal bias..."

"A duty of cooperation is imposed on every member of every agency, every departmental official and every member of the armed forces to disclose or provide to me all such documents and information as I may require. I have never had anything but cooperation in this regard."

72B. In the same report he commented on GCHQ's record keeping in terms of warrantry and authorisation:

"GCHQ also take compliance extremely seriously and the paperwork GCHQ provided was in good order and I found no slips."

72C. The Commissioner also noted that he had spent a day at GCHQ looking at the system by which GCHQ manages its internal approvals and additions, and questioning the staff who undertake the approvals and the CNE activity, in order to understand what consideration was being given at each stage of the process to protecting privacy, and what was done with any product from CNE operations. The Commissioner concluded:

"My under the bonnet inspection in December provided me with a greater understanding of how GCHQ's internal approvals apply to section 7 class authorisations. I was satisfied with the formality of the audit trail and the level of consideration that was given to each operation; it was clear to me that a great deal of thought was going into the process..."

"GCHQ primarily operate under class authorisations and have very few specific section 7s. They provide for my oversight the internal approvals they make under each class authorisation and have implemented my recommendation to ensure that the paperwork reflects that these approvals are only valid as long as the class authorisation is in place. They are approved by a GCHQ senior official but if there is any additional sensitivity or

political risk it will only be signed after a senior Foreign Office official or the Foreign Secretary has been consulted and agreed the operation is appropriate. I have made it clear that the senior official cannot authorise necessity and proportionality; this decision must be made by the Secretary of State and cannot be delegated.”

“GCHQ’s internal approvals are supplemented by what they call an “addition”. To help me gain a better understanding I spent a day in GCHQ:

- Looking more closely at the system;
- Questioning the staff who undertake the approvals; and
- Questioning the staff who undertake the activity.”

“I wanted to be clear what consideration was being given to protecting privacy at each stage of the process and what was done with any product obtained. I stressed to them the importance I place on filters which help avoid any unnecessary intrusion.”

“I was impressed with the formality of the audit trail and the level of consideration; it was clear to me that a great deal of thought was going into assessing the necessity for the activity in the national interest and to ensure privacy was invaded to the least degree possible. In future I recommended that these additions are included in the list of operations provided to me to allow me to select for closer examination and also to ensure I have a full understanding of the scale of operations in GCHQ.”

73. This recommendation has been implemented.

d) Oversight by the Intelligence and Security Committee of Parliament

The Committee

74. GCHQ is responsible to the Secretary of State for Foreign and Commonwealth Affairs. The Secretary of State is in turn accountable to Parliament. Parliamentary responsibility for scrutiny of the activities of GCHQ falls principally to the Intelligence and Security Committee of Parliament (“the ISC”).
75. The ISC, in its original form, was established by the Intelligence Services Act 1994. On 25 June 2013 the ISC was reconstituted under the Justice and Security Act 2013 (“the JSA”). From that date onwards the JSA has provided the governing statutory framework for the ISC. In its annual report for 2012-2013 [CM1-17], the ISC stated that it welcomed the changes in the JSA and that those changes were “broadly in line with those which we ourselves had previously recommended to the Government, and which will increase accountability” (at page 83).
76. The ISC operates within the “ring of secrecy” which is protected by the Official Secrets Act 1989. It may therefore consider classified information, and in practice takes oral evidence in open and closed session from the Foreign and Home Secretaries, the three heads of the intelligence services, and their staff.
77. The heads of the intelligence services are under a general obligation to arrange for any information requested by the ISC in the exercise of its functions to be made available to it. The power to refuse such a request has been removed from the heads of the

intelligence services and now lies with Ministers alone, who can only exercise this power in certain limited circumstances.

78. In order to be able effectively to carry out its expanded remit under the JSA, the ISC's budget has been substantially increased and the ISC is in the process of recruiting further staff. This will result in a three-fold increase in the ISC's investigative capacity.

Privacy and Security: A modern and transparent legal framework

79. The ISC sets its own agenda and work programme. Following the Snowden allegations in the summer of 2013, the ISC decided to investigate an allegation made in some of those reports to the effect that GCHQ had acted illegally by accessing communications content via the US PRISM programme. On 17 July the Committee made a statement [CM1-18] which concluded that the allegation that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications was unfounded. They also concluded that it would nevertheless be proper to "... consider further whether the current statutory framework governing access to private communications remains adequate."

80. On 17 October 2013, the ISC announced that it would be broadening this review of the legislative framework governing the intelligence services' access to the content of private communications to consider, additionally, the appropriate balance between privacy and security in an internet age [CM1-19]. The result of this review, *Privacy and Security: A modern and transparent legal framework*, was published on 12 March 2015 [CM1-13]. Paragraph v of the introduction to the review says:

"Our Inquiry has involved a detailed investigation into the intrusive capabilities that are used by the UK intelligence and security Agencies. This Report contains an unprecedented amount of information about those capabilities, including how they are used, the legal framework that regulates their use, the authorisation process, and the oversight and scrutiny arrangements that apply."

81. The Committee's first key finding reads:

"We are satisfied that the UK's intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do."

82. In the report the Committee also indicated that it had been informed about the full range of Agency capabilities, how they are used and how they are authorised.

Conclusion

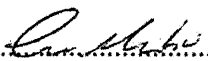
83. In this statement I have endeavoured to the best of my ability and knowledge to:

- describe the range of serious national security threats faced by the UK and its people to which GCHQ is required to assist in defending against;

- set out the requirement for Computer and Network Exploitation (CNE) capabilities to help us counter these threats, principally international terrorism, cyber attack (including from hostile state actors), and serious crime (including child sexual exploitation);
- give an account of the robust procedures for the use of GCHQ's CNE capabilities, and summarise the result of various Parliamentary, judicial and other inquiries and inspections which shows GCHQ's adherence to these strict procedures;
- describe the growing importance of CNE to the protection of the UK. Whilst it has been an important GCHQ capability for many years, its importance has been growing and is set to grow further, partly because of the growth of ubiquitous encryption which has affected GCHQ's ability to collect data for intelligence purposes by other means. It is therefore the case that without CNE capabilities GCHQ's ability to protect the British public from terrorism, cyber attack, online child sexual exploitation and a range of other serious crime would be badly diminished.

Statement of Truth

I believe that the facts stated in this statement are true.

Signed:.....

Dated: 16 November 2015

