RESPONDENTS' RESPONSE TO CLAIMANTS' SCHEDULE

The Respondents have set out in the table below their response to the Claimants' schedule of public statements on CNE served on 9 November 2015.

This schedule is served without prejudice to the following preliminary points:

1) None of the statements referred to in the schedule below constitute a substantive move away from the Defendants' neither confirm nor deny (NCND) position on CNE. As has been the consistent position of the Respondents in these proceedings, whilst the use of CNE in general terms as an intelligence gathering technique is accepted, the NCND approach must continue to apply to detailed allegations about specific CNE techniques/operations for reasons of national security.

2) The Respondents do not consider it necessary or appropriate for there to be detailed consideration as to whether these statements constitute "avowals". The Respondents do not resile from these publicly available statements/reports, the majority of which are within the scope of Mr Martin's witness statement. Importantly each of these statements has to be read in the particular context of the underlying document from which it was drawn.

3) The Respondents admitted in their Open Response in February that they carry out CNE activity and that those activities can cover a range of conduct. The Respondents have set out the legal framework within which CNE activity is authorised, and the list of issues/assumed facts cover the full range of conduct which it is alleged that the Respondents undertake pursuant to this framework. In those circumstances this schedule does not appear to add anything to the Claimants' complaints, the scope of which is well-understood and is reflected in the list of issues/assumed facts and the evidence served to date in these proceedings. Neither is there anything in the schedule which could lead to further evidence or disclosure by the Respondents.

Avowal	**Evidence**	**Respondent admits/denies**	**Respondent's reasons**
GCHQ carries out CNE within the UK	ISC, p. 67	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	The relevant domestic legal regime (the Equipment Interference Regime) was set out in the Respondents' Open

			Response dated 6 February 2015 and the EI Code of Practice. It is clear from the Equipment Interference Regime and the Code that CNE may be carried out within the UK.
GCHQ carries out CNE outside UK	ISC, p. 67; Investigatory Powers Bill Factsheet – Bulk Equipment Interference	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	The relevant domestic legal regime (the Equipment Interference Regime) was set out in the Respondents' Open Response dated 6 February 2015 and the EI Code of Practice. It is clear from the Equipment Interference Regime and the Code that CNE may be conducted outside the UK.
GCHQ uses the term "CNE"	ISC, p. 67	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	The ISC statements have been in the public domain since 12 March 2015.
In 2013, about 20% of GCHQ's intelligence reports contained information derived from CNE	Investigatory Powers Bill Factsheet – Bulk Equipment Interference; Investigatory	The Respondents accept the accuracy of this statement.	This is consistent with the ISC Report in which it was explained that, during 2013, a

	Powers Bill Factsheet – Targeted Equipment Interference (*cf*. ISC, p. 67, where the same figure is redacted)		significant number of GCHQ's intelligence reports contained information that derived from IT operations against a target's computer or network.
GCHQ has disclosed specific examples of CNE operations to the ISC	ISC, p. 67	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	Parliamentary responsibility for scrutiny of the activities of GCHQ falls principally to the ISC, and any disclosures made to the ISC were consistent with the exercise of the Committee's functions.
GCHQ undertakes "persistent" CNE operations, where an implant "resides" on a computer for extended period	ISC, p. 67 n. 183	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	The ISC statements have been in the public domain since 12 March 2015.
GCHQ undertakes "non-persistent" CNE operations, where the implant expires at end of user's internet session	ISC, p. 67 n. 183	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	The ISC statements have been in the public domain since 12 March 2015.
CNE operations undertaken by the Agencies include operations	ISC, [173]	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	Footnote 6 of the EI Code of Practice published on 6

against a specific device			February 2015 makes clear that ““Equipment” may include, but is not limited to, computers, servers, routers, laptops, mobile phones and other devices.”
CNE operations undertaken by the Agencies include operations against a computer network	ISC, [173]	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	Footnote 6 of the EI Code of Practice published on 6 February 2015 makes clear that ““Equipment” may include, but is not limited to, computers, servers, routers, laptops, mobile phones and other devices.”
CNE operations undertaken by the Agencies include operations against neither a specific device nor a computer network	ISC, [173]	The ISC Report indicates that IT operations undertaken by the Agencies include operations against a specific device, a computer network and other unspecified IT targets. The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	Footnote 6 of the EI Code of Practice published on 6 February 2015 makes clear that ““Equipment” may include, but is not limited to, computers, servers, routers, laptops, mobile phones and other devices.”

GCHQ has obtained warrants under Section 5 ISA to authorise CNE	ISC, [174]	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	The relevant domestic legal regime (the Equipment Interference Regime) was set out in the Respondents' Open Response dated 6 February 2015 and the EI Code of Practice. It is clear from the Equipment Interference Regime and the Code that warrants may be obtained under section 5 ISA to authorise CNE.
GCHQ has obtained authorisations under Section 7 ISA to undertake CNE abroad	ISC, [177]	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	The relevant domestic legal regime (the Equipment Interference Regime) was set out in the Respondents' Open Response dated 6 February 2015 and the EI Code of Practice. It is clear from the Equipment Interference Regime and the Code that authorisations may be obtained under section 7 ISA to

			undertake CNE abroad.
In 2013, GCHQ undertook operations under Section 7 to interfere with computers overseas	ISC, [178]	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	The ISC statements have been in the public domain since 12 March 2015.
GCHQ's operations to interfere with computers overseas in 2013 varied considerably in both scale and impact	ISC, [178], n. 179	The Respondents accept the accuracy of the ISC statements mentioned in the schedule.	The ISC statements have been in the public domain since 12 March 2015.
GCHQ had five section 7 class-based authorisations in 2014	Anderson 6.27	The Respondents accept the accuracy of the Anderson statements mentioned in the schedule.	The Anderson statements have been in the public domain since June 2015.
GCHQ had section 7 class-based authorisations to interfere with computers, mobile phones and other types of electronic equipment in 2014	Anderson 6.27	The Respondents accept the accuracy of the Anderson statements mentioned in the schedule.	The Anderson statements have been in the public domain since June 2015.
GCHQ is responsible for developing the National Technical Assistance Centre's CNE capabilities	Anderson 7.29	The Respondents accept the accuracy of the Anderson statements mentioned in the schedule.	The Anderson statements have been in the public domain since June 2015.
"Bulk equipment interference" is	Draft Bill Guide, [36(c)]	The Respondents do not accept	Paragraph 36(c) of the Draft Bill

increasingly used to access data from computers		that the alleged "avowal" accurately reproduces the text at paragraph 36(c) of the Draft Bill Guide.	Guide states "….equipment interference" is increasingly used to access data from computers.
The government considers that it already has the equipment interference powers provided in the draft Bill. These include powers to authorise equipment interference under bulk warrants.	Foreword from Home Secretary to Draft Investigatory Powers Bill	The Respondents cannot locate the alleged "avowal" in the Foreword.	The sole reference to equipment interference in the Foreword appears in the second paragraph: "Powers….[to] interfere with equipment are essential to tackle child sexual exploitation, to dismantle serious crime cartels, take drugs and guns off our streets and prevent terrorist attacks."
Sensitive and intrusive techniques for interference with electronic equipment (e.g. computers, smartphones) are available to the security and intelligence agencies	Draft Bill Guide, [29]	The Respondents accept the accuracy of this statement.	The Draft EI Code of Practice provides guidance on the use of CNE by the Intelligence Services, and has been in the public domain since 6 February 2015.
The Agencies have developed	Impact Assessment for	The Respondents accept the	

techniques to gain access to computers, devices and other web-based activities	Investigatory Powers Bill: Equipment Interference, pp. 1, 5	accuracy of this statement.	
EI operations may involve using someone's login credentials to gain access to information	Impact Assessment for Investigatory Powers Bill: Equipment Interference, p. 5	The Respondents accept the accuracy of this statement.	The range of activities that may comprise CNE was set out in the Respondents' Open Response dated 6 February 2015. Specific reference was made to the use of login credentials to gain access to information, and to exploiting vulnerabilities in software to gain control of devices or networks.
EI operations may involve exploiting vulnerabilities in software to gain control of devices or networks	Impact Assessment for Investigatory Powers Bill: Equipment Interference, p. 5	The Respondents accept the accuracy of this statement.	The range of activities that may comprise CNE was set out in the Respondents' Open Response dated 6 February 2015. Specific reference was made to the use of login credentials to gain access to information, and to exploiting

			vulnerabilities in software to gain control of devices or networks.
Current legislation is used to acquire personal data by both targeted and bulk EI	Impact Assessment for Investigatory Powers Bill: Equipment Interference, p. 7	The Impact Assessment sets out the costs, benefits and impact of the equipment interference provisions in the draft Bill. The assessment is accordingly concerned with the question whether the draft Bill contains new powers (as the last sentence of section C makes clear). The sentence comprising the alleged "avowal" should therefore have stated that current legislation can be used (rather than is used) to acquire personal data by both targeted and bulk EI. The Respondents accept that current legislation can be used to acquire personal data by	

		both targeted and bulk EI. However consistently with all the other overarching documents issued at the same time as the draft Bill, in particular the Factsheet for Bulk Equipment Interference, the Respondents neither confirm nor deny whether bulk EI as set out in the Bill has ever been carried out.	
Powers under the ISA are used for EI to acquire "private data"	Impact Assessment for Investigatory Powers Bill: Equipment Interference, p. 8	The Respondents accept the accuracy of this statement.	The relevant domestic legal regime (the Equipment Interference Regime) was set out in the Respondents' Open Response dated 6 February 2015 and the EI Code of Practice.
Material obtained through EI is used to investigate and prosecute serious crime	Impact Assessment for Investigatory Powers Bill: Equipment Interference, p. 10	The Respondents accept the accuracy of this statement.	The Respondents' Open Response made clear that 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.
Material obtained through EI is used to protect UK cyber security	Impact Assessment for Investigatory Powers Bill: Equipment Interference, p. 10	The Respondents accept the accuracy of this statement.	The Respondents' Open Response made clear that 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.
The Agencies currently have an ability to obtain communications and private data through EI, both targeted and in bulk	Investigatory Powers Bill Privacy Impact Assessment, p. 9	The Respondents accept that current legislation can be used to acquire/obtain communications and private data through EI, both targeted and in bulk. However the Respondents neither confirm nor deny whether bulk EI as set out in the Bill has ever been carried	

		out.	
Bulk warrants authorise the use of EI to obtain and analyse the data of persons outside the UK	Investigatory Powers Bill Factsheet – Bulk Equipment Interference	The Respondents accept the accuracy of this statement in the context of the powers conferred by the Investigatory Powers Bill. However the Respondents neither confirm nor deny whether bulk EI as set out in the Bill has ever been carried out.	
EI is used to secure intelligence	Investigatory Powers Bill Factsheet – Bulk Equipment Interference	The Respondents accept the accuracy of this statement.	The Respondents' Open Response of 6 February 2015 made clear that CNE is used to secure valuable intelligence to enable the State to protect its citizens from individuals engaged in terrorist attack planning, kidnapping, espionage or serious organised criminality.

ISC = *Intelligence and Security Committee of Parliament. Privacy and Security: A Modern and Transparent Legal Framework* (2015)

Waller = *Report of the Intelligence Services Commissioner for 2014* (2015)

Anderson = *A Question of Trust. Report of the Investigatory Powers Review* (2015)

Draft Bill Guide = *Draft Investigatory Powers Bill: Guide to Powers and Safeguards* (2015)

19 November 2015