[redacted]

WITNESS STATEMENT OF GEOFF BLUEMEL ON BEHALF OF THE NATIONAL CRIME AGENCY

1. I am the Senior Manager for the Specialist Operations (Online) department within the National Crime Agency ("NCA"). My role involves the management of the NCA's undercover online ("UCOL") officers.

2. I am authorised to make this witness statement on behalf of the NCA.

3. I make this statement further to the Inquiry legal team's comments as to the adequacy of the generic CLOSED evidence, as at 1 August 2017.

4. I understand that CLOSED Ground G refers to operational tactics and that there are a number of sub-categories contained within that ground, one of which is sub-category **X** which specifically relates to "covert activity online."

5. Covert online activity is a new and emerging area of undercover work. Whilst there is, it is accepted, limited public knowledge regarding the fact that undercover officers <u>can</u> deploy online, the details and limitations of the tactic and the extent to which UCOL officers can infiltrate the activities of criminals online, have, to date, been protected from disclosure into the public domain. There is also a very significant difference between the limited public knowledge and suspicion that exists to date and there being official confirmation through the Inquiry that the tactics are used and the details of the same.

6. I am aware that the NCA holds a significant number of documents that relate to covert online activity that are either of potential relevance to the Inquiry or have already been identified by the Inquiry to be both relevant and necessary to the Inquiry's

[redacted]

Terms of Reference. Having reviewed these documents, I can confirm that they contain numerous sensitive details regarding covert activity online.

7. Were the details contained within these NCA documents (or wider documents that may be held across law enforcement) to be made public during the course of the Undercover Policing Inquiry, the damage to the continuation of the UCOL tactic would be significant and would undermine the ability of the NCA (and wider law enforcement partners, both in the UK and abroad) to infiltrate those offending online, something that already proves extremely difficult.

8. The purpose of this witness statement is therefore to provide detailed evidence in support of CLOSED Ground G(x).

9. The evidence contained in this statement is inevitably of a generic nature. It is anticipated that it may well be necessary to provide further evidence relating to specific risks when the Inquiry comes to focus on the potential disclosure of particular documents or passages within documents.

The undercover online (UCOL) officer

10. By way of background, a UCOL officer is defined as a nationally accredited operative who is deployed to establish and maintain relationships with an individual, network or organisation through the use of the internet with the covert purpose of obtaining intelligence, information or evidence as part of an authorised operation.

11. Online deployments are authorised pursuant to the Regulation of Investigatory Powers Act ("RIPA") 2000 and are subject to the same considerations, reviews and scrutiny as any physical undercover deployment. Indeed, some UCOL officers are also accredited to undertake offline deployments.

12. Undercover officers are only authorised to deploy online when it is necessary and proportionate to use this intrusive technique to investigate serious criminal activity.

13. All offline undercover officers now also undergo some basic online awareness training. The purpose of this training is to enable them to communicate safely and

[redacted]

securely on the internet if required during the course of any offline undercover operation.

The use of the internet by criminals

14. In very broad terms, the way the internet is used by criminals can be divided into two categories of offences:

a) **internet dependent offences** - offences that could not be committed without the internet (e.g. a denial of service attack); and

b) **internet enabled offences** – offences that are facilitated by use of the internet (e.g. the online sale of firearms).

15. These offences can be further sub-divided between those which take place on the public internet (the 'Clearnet') and those that occur on the 'Dark Web'[1].

16. The proliferation of internet enabled devices and associated apps is making it increasingly easy for 'non-technical' individuals to access illicit material, commit crime and communicate securely online. For example, for a user to access the Dark Web they only need to download the Onion Router ("TOR") browser, which is free and very straight forward to set-up and use.

17. This provides opportunities and incentives for people who do not fit the historic criminal profile to become involved in some very serious crime, [redacted] These individuals are frequently more intelligent and better educated than previous generations of criminals and in many cases otherwise lead ostensibly law- abiding lives.

18. For example, the 'traditional' street drug dealer would generally have a high expectation of encountering violence, either as the perpetrator or as a victim. However, the online drug trade virtually eradicates this risk, both for the dealer and the customer.

[1] The Dark Web is the World Wide Web content that requires specific software, configurations or authorisations to access. It allows users and website operators to remain anonymous and/or untraceable.

[redacted]

19. In addition to altering the risks they face, the internet also allows them to network, educate and share knowledge across national and international boundaries very easily. Many of the forums and websites have specific sections dedicated to advising members on how to avoid law enforcement action. It is for this reason that it is so essential that the details of the UCOL tactic (whether in terms of steps that can be taken to infiltrate online criminals or current limitations of the tactic that, if known, would be exploited) are not made public during the course of the Inquiry.

20. [redacted]
Examples are given of efforts made by criminals to expose law enforcement tactics.

21. [redacted]

22. [redacted]

23. It is evident that each time law enforcement action is successfully taken against one of these websites, the online criminal community learn from the experience and adapt their approach in an attempt to frustrate future law enforcement investigations. [redacted]
Further example is given of efforts made by criminals to expose law enforcement tactics.

[redacted]

24. Examples are given of efforts made by criminals to frustrate law enforcement tactics. [redacted]

25. [redacted]

How undercover officers are used in connection with these online threats

26. In the case of a criminal using the 'Clearnet' to commit criminal offences (e.g. a sex offender using a social media platform to groom a child), the main objective of any undercover deployment will be to gather sufficient evidence to prove that the subject has a genuine interest in children for the purposes of sexual activity. Once confirmed, enquiries will be undertaken by the investigating team to identify the offender, [redacted] The evidence gathered by the UCOL can then be used as the basis of any arrest and prosecution.

27. In these circumstances, in order to establish that an offender has a sexual interest in children, an undercover officer may be authorised to pose as another adult with a sexual interest in children, or alternatively pose as a vulnerable child. However, they must not act as an *agent provocateur*[3].

[redacted]

[3] A person employed to induce others to break the law so that they can be convicted.

[redacted]

28. Although offenders are aware that law enforcement (and vigilante groups) might use these tactics, they are forced to use the 'Clearnet' to interact because that is where their potential victims are likely to be found. [redacted]

Examples given of efforts made by criminals to avoid detection.

29. [redacted]

Examples given of UCOL deployments, tactics and associated sensitivities. It is said that to reveal these would damage use of the tactics and make it significantly more difficult successfully to prosecute online offenders.
(Gist applicable to paragraphs 29-38)

30. [redacted]

31. [redacted]

[redacted]

[redacted]

[redacted]

32. [redacted]

33. [redacted]

34. [redacted]

35. [redacted]

36. [redacted]

[redacted]

37. [redacted]

38. [redacted]

The training and continuous professional development of undercover officers

39. I am aware that, in the documents held by the NCA that are either of potential relevance to or have been held to be both relevant and necessary in the context of the Inquiry's Terms of Reference, there are many references to the training of and continuous professional development of UCOL officers. One obvious example is the recently published CSE Threat Assessment which relates to grooming, and has a specific section highlighting the challenges for UCOL deployments in the respective platforms.

40. [redacted]

[redacted]

[redacted] The training of undercover officers is constantly having to evolve to keep pace with the rapidly changing technology and offender behaviour in this area.

41. As I have stated above, the online criminal community would, if armed with this training material (were it to be exposed during the course of the Inquiry) publicise it internationally in an effort to undermine the ability of law enforcement to infiltrate those offending online in the future.

42. I believe the contents of this statement are true.

Signed: [redacted]

Dated: 28/9/17.