

OFFICIAL

Statement made on behalf of: The Commissioner of Police of the Metropolis

Witness: MICHAEL KILLEEN

Statement No: 3

Exhibits Referred to: N/A

Date Statement Made: 3 January 2017

IN THE MATTER OF: PUBLIC INQUIRY INTO UNDERCOVER POLICING

Witness: MICHAEL KILLEEN

Occupation: Police Officer

I believe the facts stated in this witness statement are true

Signed... 

Dated...  3.1.2017

Preface regarding update to statement

On 22 June 2016 I made a statement of 60 paragraphs. On 20 September 2016 I made amendments to the statement, extending it to 83 paragraphs. That statement read as follows:

Introduction

1. I am Temporary Detective Superintendent Michael Killeen currently seconded to the National Counter Terrorism Policing Operations Centre (NCTPOC) based in London.

OFFICIAL

2. I make this statement in response to the Inquiry's tenth Rule 9 request dated 18 May 2016.
3. I have served as a police officer for 27 years. My service has included secondments to the National Crime Squad and Serious Organised Crime Agency. Between 2014 and 2016, I held the rank of Detective Chief Inspector as Head of Intelligence for Humberside Police.
4. My current role in the NCTPOC is Head of Intelligence, with responsibility for the management of domestic extremism and counter terrorism intelligence.
5. I have been in post with the NCTPOC since February 2016. As a consequence of my recent appointment I have worked closely with an experienced colleague, [REDACTED], to answer the Inquiry's questions. [REDACTED] joined the NPOIU on 3 January 2006 as a Higher Analyst. [REDACTED] was subsequently promoted to Senior Analyst and Head of the [REDACTED] which he set up. [REDACTED] is explained at paragraph 34(iv). [REDACTED] is currently the Head of Digital Intelligence with responsibility for [REDACTED] and the Counter Terrorism Internet Referral Unit. He joined the Metropolitan Police service in 2001.
6. I have also liaised with Detective Sergeant [REDACTED]. He is the NCTPOC officer with responsibility for the National Humint Team (NHT), also known as the Strategic Sensitive Source Unit. The role of this team is explained at paragraph 28.
7. I have also liaised with Detective Sergeant Person B [REDACTED] in relation to the National Special Branch Intelligence System (NSBIS) database. The database is explained at paragraphs 31 to 33. He is the NCTPOC officer with responsibility for indexing intelligence on the database and

OFFICIAL

the implementation of the Review, Retention and Disposal (RRD) policy.

Background

8. Before addressing each of the Inquiry's questions, it is necessary to set out briefly the background to the development of domestic extremism and strategic protest policing in the UK.
9. In 1986, the Special Branch network set up the Animal Rights National Index (ARNI) in response to growing concerns about animal rights extremism in the UK. In 1999, this unit was developed into the National Public Order Intelligence Unit (NPOIU). The NPOIU's role was to manage all domestic extremism intelligence. Between 1999 and 2006, the NPOIU was governed by the MPS.
10. In 2004, Cambridgeshire Police established the National Extremism Tactical Coordination Unit (NETCU) to liaise with and to offer preventative advice to industries subject to domestic extremism campaigns.
11. In the same year, a steering group was created to assist with the governance of the NPOIU. The group consisted of an ACPO member from each region. It met quarterly. In the same year, a National Coordinator for Domestic Extremism (at Assistant Chief Constable rank) was appointed to ensure greater coordination between the NETCU and the NPOIU.
12. In 2005, ACPO formed the National Domestic Extremism Team (NDET) responsible for co-ordinating police operations and investigations against domestic extremists. In 2006, the three units came under the governance of ACPO. As I have indicated, prior to that

OFFICIAL

time the NPOIU was managed by the MPS, the NETCU by the Cambridgeshire Police and the NDET by ACPO.

13. In 2010, the three national units (NPOIU, NETCU and NDET) merged to become the National Domestic Extremism Unit (NDEU). This was a single unit based in one office with responsibility for domestic extremism intelligence. In the same year, the NPOIU steering group was disbanded. In January 2011, the ACPO Chief Constables' Council ratified the decision for the Metropolitan Police Service (MPS) to become the lead force for the NDEU under the governance of SO15 (Counter Terrorism Command). From that date, the MPS took over responsibility for domestic extremism intelligence from ACPO.
14. The merger was designed to fulfil the strategic requirement for Public Order and Domestic Extremism intelligence, to improve national coordination, to reduce costs and duplication between the three units and to ensure effective and efficient working practices. The new structure had a smaller team undertaking investigation support and development (the old NDET function) and a much smaller team conducting industry liaison (the old NETCU function).
15. Following the merger, the NDEU did not have the capacity to conduct undercover policing operations. Local forces became responsible for conducting their own undercover policing operations. The NDEU maintained the NPOIU's intelligence collating, analysis and strategic overview functions.
16. On 1 May 2013, the NDEU was re-named the National Domestic Extremism and Disorder Intelligence Unit (NDEDIU). The role of NDEDIU and its successor units is set out at paragraphs 21 to 29 below.

OFFICIAL

17. In 2015, the NDEDIU was renamed the National Counter Terrorism Intelligence Unit (NCTIU).
18. On 8 January 2016, the NCTIU was renamed the National Counter Terrorism Domestic Extremism Intelligence Unit (NCTDEIU).
19. On 4 April 2016, the NCTDEIU was permanently renamed the NCTPOC. Following the re-naming and re-structuring of the NDEDIU between 2015 and 2016, the NCTPOC absorbed the NDEDIU's responsibilities for domestic extremism. The NCTPOC has additional responsibility for Counter Terrorism that did not form part of the NDEDIU's remit.
20. I will now address each question asked by the Inquiry.

1) Describing the purpose, role and remit of the NDEDIU, and in particular its involvement in or use of undercover policing now and in the past;

21. As will now be clear, the NDEDIU no longer exists. However, the NCPTOC, the NDEDIU's successor unit, retains the same purpose, role and remit as the NDEDIU in relation to domestic extremism. The following explanation as to the NDEDIU therefore applies to the NCPTOC.
22. In summary, the NDEDIU was responsible for receiving from local police forces, storing, interpreting, analysing and disseminating to local police forces, domestic extremism-relevant intelligence. The NDEDIU would also support local police forces in relation to domestic extremism matters and provide a strategic overview to both police forces and Her Majesty's Government about domestic extremism in the UK.

OFFICIAL

23. The NDEDIU had no involvement in undercover policing operations. However, it received intelligence reports from police forces, which may have originated from undercover policing operations. The reports would be sent to the NDEDIU for the purposes of including them in the NSBIS database and to inform the NDEDIU's analysis of domestic extremism matters. The reports sent to the NDEDIU would be drafted in such a way that the NDEDIU would not know the source of the intelligence. The NDEDIU would therefore not know or have any records to indicate whether intelligence supplied by local police forces was the product of undercover policing operations.
24. In more detail, the overarching aim of the NDEDIU was to reduce and wherever possible remove the threat of crime, criminality and public disorder arising from Domestic Extremism and Disorder affecting the UK and our international partners. The unit operated along a continuum from public order through to domestic extremism and terrorist activity.
25. The role of the NDEDIU was to:
- Provide the national strategic domestic extremism and strategic protest threat picture for the police and Whitehall partners.
 - Co-ordinate and facilitate domestic extremism and strategic protest intelligence gathering.
 - Maintain full visibility of the Domestic Extremism & Disorder (DE&D) threat picture nationally and the police response to it.
 - Provide tactical analysis in relation to open source and social media intelligence from [REDACTED]
 - Regular assessment products for law enforcement, partners & government stakeholders.
 - Provide strategic and tactical support to UK police in relation to large scale/cross border protest.
 - Make sense of the evolving DE&D threat picture to inform future policy and operational response.

OFFICIAL

- Explain the impact that the policing response has made in countering the DE&D threat.
26. The policing purpose of the NDEDIU was to identify domestic extremists and to protect public safety by maintaining oversight of strategic protest, groups or individuals motivated by political conviction.
27. Disorder for NDEDIU policing purposes was described as strategic protest that may:
- (i) significantly affect community tensions;
 - (ii) attract significant counter protest;
 - (iii) cause economic or reputational impact to the UK;
 - (iv) require the deployment of significant police resources; or
 - (v) is otherwise set by the NDEDIU strategic intelligence requirement.
28. The National Humint Team (NHT), also known as Strategic Sensitive Source Unit formed part of the NDEDIU and continues to form part of the NCTPOC. The team was formed from the NPOIU Source Management Unit. The role of the NPOIU Source Management Unit (SMU), which remains the same today, is the co-ordination, strategic direction, de-confliction, tasking and funding of national Domestic Extremism Confidential Human Intelligence Sources (CHISs). Such CHISs did not and does not include undercover police officers (UCOs). The SMU was not involved in undercover policing operations.
29. UCOs were managed by the NPOIU Special Projects Team and their intelligence was disseminated through the NPOIU Confidential Unit. Both of these teams were separate to the SMU; however, they were all under the command of the same Detective Chief Inspector. The NDEDIU did not have an equivalent unit as it did not run undercover operations. No one currently working in the NCPTOC has knowledge of undercover policing operations conducted by the NPOIU.

OFFICIAL

2) Listing all operations that have been conducted by the NDEDIU, or in which the NDEDIU has had involvement, which have involved the use of undercover policing (to any extent);

30. As noted above at paragraph 23, the NDEDIU and its successor units did not conduct and were not involved in undercover policing operations. I have reviewed retained NDEDIU operational records and I am not aware of any operation that involved undercover policing. NDEDIU operations included providing support to local forces in relation to domestic extremism and public order incidents. However, as noted above, when providing intelligence or asking for NDEDIU assistance police forces would not indicate to the NDEDIU whether undercover policing was involved. In order to ascertain whether intelligence held by NDEDIU originated from undercover policing, it would be necessary to make enquiries with local police forces.

3) Describing how NDEDIU records are stored and organised, including

- a. A list of all the electronic and hard-copy document repositories which currently hold NDEDIU material – please ensure that the statement identifies any repositories which are considered particularly likely to contain material relevant to the terms of reference, and similarly any which are considered unlikely to contain such material; and*
- b. In relation to electronic repositories, an explanation of whether that repository is a stand-alone system or not, whether there is any back-up system or data store, and which categories of staff and/or officer have access to it;*

31. All NDEDIU intelligence records are stored electronically on the National Special Branch Intelligence System (NSBIS) database. It is

OFFICIAL

necessary to set out some background as to the history of this database.

32. In January 2012, Her Majesty's Inspectorate of Constabulary (HMIC) published a report that concluded that information was being unnecessarily retained on the NDEDIU NSBIS database. The database was started in 2006.¹ This led to the introduction of a new NDEDIU RRD policy for recording public order intelligence and a full review of the NSBIS database to ensure that it was necessary to retain each piece of intelligence. In April 2013, HMIC conducted an audit of records created since the policy was implemented in April 2012. The report concluded that there was compliance with the policy and the retention of new intelligence was necessary and justified. In June 2013, HMIC published a second report, which approved the new NDEDIU policy and found that some records still needed to be reviewed against the new criteria for retention.² The review therefore continued into 2014. The new policy as recommended and approved by HMIC resulted in the deletion of a significant number of records between 2012 and 2014.
33. In May 2014, the NDEDIU started a new NSBIS database that initially contained no data. Officers manually migrated intelligence records and reports from the old database to the new 'live' database in accordance with the NDEDIU policy on the proper retention of information. The original database became known as the Legacy database. Following the creation of the new instance of the database the RRD policy was no longer applied to the Legacy database and consequently no further information should have been deleted.
34. The following is a list of all the electronic and hard-copy document repositories which currently hold NDEDIU material:

¹ A review of national police units which provide intelligence on criminality associated with protest.

² A review of progress made against the recommendations in HMIC's 2012 report on the national police units which provide intelligence on criminality associated with protest.

OFFICIAL

- i) The Legacy version of the NSBIS database decommissioned in 2014 contains intelligence that may be pertinent to the Inquiry's terms of reference. This is because the intelligence may have resulted from undercover policing operations conducted by local forces. The local forces are likely to have retained the intelligence and information about the underlying investigation, including whether it involved undercover policing (subject to local RRD policies and Management of Police Information requirements).
- ii) The new instance of the NSBIS database commissioned in 2014 may also contain material pertinent to the Inquiry's terms of reference for the same reason.
- iii) The thematic desks (for example, in relation to animal rights extremism) keep research records and intelligence under development on a shared drive of NSBIS. Any intelligence is also inputted to the NSBIS database. The shared drive could also therefore include the product of undercover policing operations.
- iv) The [REDACTED] contains open source research relevant to domestic extremism which is held on a separate server to NSBIS. [REDACTED] is highly unlikely to hold any material relevant to the Inquiry's terms of reference as it consists of open source material.
- v) The National Humint Team (NHT), also known as the Strategic Sensitive Source Unit, hold hard copy and electronic document repositories but this unit has not and is not concerned with undercover policing matters. The electronic material does not include material relevant to the Inquiry's terms of reference. The

OFFICIAL

hard-copy material may contain material relevant to the Inquiry's terms of reference (as detailed below at paragraphs 38 to 39).

35. All the electronic databases, shared drivers and servers are stand-alone.
36. [REDACTED] and the new instance of the NSBIS database are backed up weekly. All NCTPOC staff are vetted to a minimum of SC level, and have access to these databases. They can amend and delete entries as part of normal day to day usage. Any such amendment or deletion will be auditable and records will show who made the amendment or deletion, and when. A Detective Sergeant on the unit is responsible for all deletions in accordance with the HMIC-approved RRD policy.
37. The old instance of the NSBIS database is no longer in use and is retained as a legacy database. It therefore has no back up system. It remains searchable by one member of civilian support staff for the purposes of responding to Data Protection Act 1998 and Freedom of Information Act 2000 enquiries and the NCTPOC's IT manager. It has also been made available to the Operation Herne and MPS Public Inquiry teams. No-one else has access to the Legacy database. [update: please see paragraph 71 below]
38. As noted above at paragraph 34 v), the NHT within the NCTPOC may hold hard copy material relevant to the Inquiry's term of reference. The NHT have two storage safes held at a secure location. They are identified as Cabinet 20 and Cabinet 21. Cabinet 20 contains 374 paper folders and Cabinet 21 contains 154 folders. Each folder contains paper documents in relation to individual CHISs. The paper documents held within each file vary in content; however, in general it is administrative information such as funding, minutes of meetings, performance and cancellation of the CHIS. The dates of these folders range from 1995 to 2015. It is unlikely that these files concern

OFFICIAL

undercover police officer CHISs; however, given that the date range extends into the operational period of the NPOIU, the cabinets have been referred to ACPIT and Operation Filesafe for review as to whether they cabinets contain any of the material relates to the Inquiry's terms of reference.

39. In addition, there is a further safe identified as Cabinet 35 held in the NCTPOC Detective Chief Inspector's office at the same secure location. This may hold data of undercover policing operations conducted by the NPOIU, including authorities for deployments. This cabinet has been referred to ACPIT and Operation Filesafe for review as to whether any of the material relates to the Inquiry's terms of reference.
40. Cabinet 35 can only be accessed by me and the NCTPOC Detective Chief Inspector. The material is held in a locked safe appropriate to its Secret security classification. Cabinets 20 and 21 are subject to the same restricted access, save that DS [REDACTED] also has access in his capacity as a member of the National Humint team for the purposes of accessing records about non-UCO CHISs.

4) Describing the extent to which the NDEDIU took over the role and functions of the NPOIU upon its closure, and the extent to which the NDEDIU continues to fulfil that role/carry out those functions;

41. The answer to this question has been set out in the 'Background' section at paragraphs 8 to 20 and in the answer in response to question 1.

5) Explaining the extent to which the NDEDIU took possession of the records of the NPOIU upon its closure;

OFFICIAL

6) To the extent that such records came into the possession of the NDEDIU, explaining where those records have been held since that time – please ensure that the witness statement mentions all locations in which such documents are currently understood to be held, as well as any repositories that have been used historically by the NDEDIU to hold such material but which are no longer in use, and include both electronic and hard copy repositories;

42. It is convenient to address questions five and six together.
43. As far as I am aware, the only electronic records that the NDEU and its successor units took possession of from the NPOIU was the 2006 instance of the NSBIS database. The original instance of NSBIS was commissioned for the NPOIU in August 2006. The NDEU inherited this database and continued to use this system until it was replaced with the new instance in 2014. As noted above, the Legacy version remains available to the NCTPOC, ACPIT, Operation Herne and the Inquiry.
44. I do not know whether the NDEU and its successor units took possession of hardcopy NPOIU files. Some of the documents described at paragraphs 38 to 39 may have originated from the NPOIU. Save as outlined in those paragraphs the NCTPOC does not hold any hard copy files relating to the NPOIU. Furthermore, the NDEDIU did not and the NCTPOC does not hold hard copy intelligence files as all intelligence is stored electronically.
45. All hard copy and electronic records described above are held at secure NPCC premises in London. The hard copy documents have been held at that location since 2010.

OFFICIAL

(7) Describing the quantity and general nature of NPOIU material currently held in each such location;

46. In relation to the old instance of the NSBIS database, it is difficult to determine the quantity of material held as it can be unstable and difficult to interrogate; however, it is likely that the database holds the vast majority of domestic extremism intelligence submitted to the unit between 2006 and 2014.
47. The new instance of NSBIS also contains material relating to domestic extremism and strategic public order. The database currently holds in excess of [REDACTED] intelligence reports and includes [REDACTED] nominals.
48. The hard copy material potentially originating from the NPOIU has been detailed at paragraphs 38 to 39.

(8) In relation to any electronic repository of information within the control of the NDEDIU which currently holds NPOIU material, explaining whether that repository is a stand-alone system or not, whether there is any back-up system or data store, and which categories of staff and/or officer have access to each repository;

49. This question has been answered at paragraphs 31 to 40.

9) To the extent that NPOIU records did not come into the possession of the NDEDIU, explaining – to the best of the knowledge and belief of the NDEDIU – what became of those records;

50. The NCTPOC does not know what became of NPOIU records that did not come into its possession.

OFFICIAL

10) Explaining what steps are in place within the NDEDIU to ensure that documents which are of potential relevance to this Inquiry are preserved (i.e. not destroyed or altered, routinely or otherwise); what steps have been taken to address the risk that individual officers or staff may deliberately seek to destroy or amend parts of the record; and what steps have been taken to ensure that any such attempt will be prevented or detected.

51. I am aware that Detective Superintendent Neil Hutchison's witness statement made in response to the UCPI's eighth Rule 9 request makes reference to the steps taken to preserve NPOIU material. I have reproduced the relevant sections of that statement here for ease of reference.

52. At paragraph 18 of his statement, DSU Hutchison states: *"I also considered, from an early state, how to ensure such potentially relevant material would be retained. My initial considerations were as follows:...(iii) Material relevant to the operations of the National Public Order Intelligence Unit was secured by Op Herne and MPS Directorate of Legal Services. This material was held in a secure environment with access restricted to staff attached to Op Herne and DLS."*

53. At paragraph 59 of that statement, he adds a clarification to paragraph 18: *"In 2014 I was aware that a considerable quantity of paper files and digital storage devices relating to NPOIU operations was held by MPS Directorate of Legal Services and Op Herne. I do not suggest that all material relevant to that units operations had been seized by Op Herne or was held in DLS at that time. Material relevant to NPOIU operations has been identified and seized by Op Herne since 2013, although the majority of NPOIU digital exhibits were seized in 2014. There will still be material relevant to that unit held by the MPS which has not yet been identified and located. Material relevant to the unit's operations will exist within MPS databases such as IMOS. The limited review of*

OFFICIAL

NPOIU operations conducted to date means that I am unable to confirm at this point whether all relevant material has been seized and is securely stored. For example, it appears that not all NPOIU material held in deep storage is clearly marked as having originated from that unit. The material can be searched for under its operation name but Op Herne are still in the process of identifying all operations linked to the NPOIU. The original Terms of Reference for Op Herne agreed on 21st June 2013 included investigation of one area of NPOIU operations directly linked to the MPS. It was not until 12th October 2015 that Op Herne's Terms of Reference were amended to include an objective review of all NPOIU operations (D10203). Progress on this review has been very limited to date due to a lack of available resources."

54. At paragraph 48 DSU Hutchison explains the steps taken to address the risk that individual officers or staff may deliberately seek to destroy or amend parts of the record. At paragraph 48(ii) he states: *"Material related to NPOIU operations - In February 2013 Op Herne obtained the NPOIU material relating to [gist: a specific operation]. Op Herne took possession of all other currently known NPOIU material in June 2015. A schedule has been completed of the content of this material. Relevant material was located by Op Herne in MPS deep storage archives, MPS Directorate of Legal Services local archive, IMOS and local archives previously used by the NPOIU and now controlled by the NDEDIU. In October 2015, Op Herne agreed with the MPS to add the investigation of NPOIU operations to its terms of reference. Op Herne has created a digital copy of paper archives of NPOIU material on the secure Holmes / Altia case management system described above. Digital exhibits relevant to the NPOIU are held in Op Herne's secure exhibit system.*
55. At paragraph 63, DSU Hutchison added an update: *"Update to paragraph 48 (ii) of my previous statement. In this paragraph I provide a date by which Op Herne took possession of all other currently known*

OFFICIAL

NPOIU material. At the time of writing my previous statement this was the information I had. I am now aware that further NPOIU related material was recovered by Op Herne after this date.”

56. The NCTPOC has complied with instructions received from Operation Filesafe, in particular that no material of potential relevance to the Inquiry's Terms of Reference should be deleted, destroyed or amended. This message has been disseminated by email to all NCTPOC staff. There have been no reported breaches of this instruction.
57. In accordance with those instructions, potentially relevant hard copy documents in Cabinets 20, 21 and 35 have been referred to ACPIT and Operation Herne for review. The security arrangements for that hardcopy material are set out at paragraph 39 to 40.
58. In relation to the the Legacy instance of the NSBIS database, and as described above at paragraph 37, only two members of NCTPOC staff are permitted access to the database and no information deletion is permitted. As the Legacy instance is inaccessible to all but two members of staff the risk of data being deleted has been minimised. [update: please see paragraph 71 below]
59. The circumstances in which information was deleted from the Legacy database in the past are detailed at paragraphs 32 to 33. As noted above, the strict restrictions on access are a safeguard against record deletion. Any attempts to amend an entry by an individual would be captured in the audit history for that entry.
60. In relation to the current instance of the NSBIS database, the access arrangements for the NCTPOC staff are set out at paragraph 36. A HMIC-approved RRD policy remains in place for the new database. Any records routinely deleted in accordance with that policy that may

OFFICIAL

(unbeknown to the NCTPOC) have resulted from undercover policy is likely to be retained on the Legacy database or with local forces (who will know whether undercover policing was involved in gathering the submitted intelligence). As noted above, any amendments or deletions will be recorded on the database, which acts as a safeguard against inappropriate amendments or deletions.

Additions dated 20 September 2016

The Undercover Policing Inquiry ('UCPI') have asked me to address a number of questions that arise from this statement in 10 numbered paragraphs of the 13th rule 9 request made to the MPS (referred to as 'rule 9(13)'). My responses to those questions are addressed below, as a continuation to my earlier statement.

Rule 9-13 paragraph 1:

With reference to paragraph 32 of the statement – please explain what the “new NDEDIU RRD policy for recording public order intelligence” said about what information should be retained and what information should be deleted.....What if any audit trail exists of the deletion of information from what is known as the Legacy database, between 2012 and 2014. What if any trace remains of records deleted in this manner?

61. Paragraph 32 refers to the 2012 RRD policy for the NDEDIU. I was informed of the 2012 policy by my colleague [REDACTED]. As stated at paragraph 5 above, I worked closely with him in producing this statement. I did not read the 2012 NDEU policy referenced in HMIC Review June 2013. It has not been relevant to my role (set out at paragraph 1 above) for the reasons set out at paragraph 79 below. I have not been able to apprise myself of this 2012 NDEU policy before the date for responding to rule 9-13. For these reasons I do not have the information to respond to the questions in paragraph 1 of rule 9-13. I understand that the MPS will seek to provide an answer to this paragraph to the UCPI as soon as possible.

Rule 9-13 paragraph 2:

With reference to paragraph 33 – it is suggested that following creation of the new NSBIS database no further information on the Legacy database “should have been deleted”; please confirm what if any checks have been conducted,

OFFICIAL

or could be conducted, in order to ascertain whether any material has in fact been deleted from the Legacy database since 2014.

62. I am not aware of any checks having been conducted to ascertain whether material has been deleted since 2014. There are three individuals who may know whether checks have been conducted. The terms of rule 9-13 prevent me from asking one of these three individuals. The other two individuals are retired. I understand the MPS is attempting to make contact with either or both of them to ascertain whether they can provide further relevant information.

Rule 9(13) paragraph 3:

With reference to paragraphs 33, 46-47, and 60 – please confirm whether the “NDEIU policy on the proper retention of information” is the same as, or different from, the policy referred to at question 1 above. Please explain what this policy said about which intelligence records and reports were to be migrated to the new NSBIS database from the old NSBIS database. In particular, please confirm whether all such records were migrated across to the new database or only some records; if only some records were migrated across, please ensure that your answer explains what criteria were applied in order to select which were to be migrated. The Inquiry notes that at paragraphs 46-47 no explicit mention is made as to whether the quantity of material on the new NSBIS database includes material that was migrated from the Legacy database, or not; please clarify this point. Following from the answers to those questions, please clarify the meaning of “likely” at paragraph 60, where it is asserted that that [sic] records held on the current NSBIS database are “likely to be retained...” on the Legacy database.

63. Question 1 (and paragraph 32 of my statement) refers to the 2012 NDEU RRD policy introduced following the 2012 HMIC inspection. Paragraphs 33 and 60 of my statement refer to the NDEIU RRD policy from 2014 that accompanied the new instance of the NSBIS database. I understand this is different to the 2012 NDEU RRD policy

OFFICIAL

referred to at paragraph 32. Paragraphs 46-47 do not refer to the "*NDEDIU policy on the proper retention of information*".

64. The 2014 policy, referred to at paragraphs 33 and 60 above has a section entitled "*The RRD Process – Interim Data Cleansing*" starting at page 6. This section sets out the criteria to be undertaken in transferring data to the new instance of NSBIS. In short, RRD was to be undertaken in accordance with the principles of the 2014 policy on material on the old instance of NSBIS before it was transferred to the new instance of NSBIS to ensure data retention was proportionate and lawful. The process to be undertaken is set out in the policy. I understand this policy has already been sent to the UCPI. The individuals in charge of this migration at the time are likely to know further details of how this was implemented. I understand that the MPS is seeking to obtain a response from the relevant individuals to see if they can provide further relevant information.
65. I understand that the new instance of NSBSIS will contain records from the old instance.
66. With regard to paragraph 60: records routinely deleted that resulted from NPOIU undercover policing will have originated before 2010 as this is the time that public order undercover policing under the NPOIU ceased (see paragraph 15 above). These documents would have been created before the transfer from the old NSBIS instance to the new, in 2014. As the old NSBIS instance remains available, this information will be retained on it regardless of whether it was (1) transferred onto the new NSBIS database in 2014 or (2) deleted routinely since then.
67. Paragraph 60 uses the word 'likely' because I cannot rule out that new information provided to NCTPOC (under the current or previous names) after 2014 by police forces or partner agencies is in fact the result of undercover policing. Such (post-2014) material may have

OFFICIAL

been deleted if it falls within the RRD policy. However, NCTPOC has no method of ascertaining whether such material relates to undercover policing. Only the originating forces would have that information for the reasons explained at paragraphs 73-74 below. For this reason I believe paragraph 60 represents the position accurately.

Rule 9-13 paragraph 4:

At paragraph 34(i) it is suggested that the Legacy database contains intelligence that "may have resulted from undercover policing operations conducted by local forces". However, with reference to paragraph 43, the Inquiry understands that the Legacy database was originally commissioned for the NPOIU. Please confirm whether the Legacy database also holds material related to undercover policing carried out by the NPOIU.

68. The Legacy database does hold information related to undercover policing carried out by the NPOIU, though it is difficult to trace that material for the reasons set out at paragraphs 73-74 (which I understand applied to information received from NPOIU sources) below.

Rule 9-13 paragraph 5:

Please confirm whether the effect of paragraph 34(iii) is that anything kept by the thematic desks on a shared drive of NSBIS would be replicated on the NSBIS database, and therefore the shared drive does not represent a separate source of potentially relevant information. If that is not the effect, please provide further explanation.

69. This is not something within my knowledge for the reasons set out at paragraph 79 below. At present I am aware of one individual who is likely to know but the terms of rule 9-13 prevent me from asking one of this individual. I understand the MPS is attempting to provide a response to this paragraph.

OFFICIAL

Rule 9-13 paragraph 6:

With reference to paragraph 36 – please confirm whether the records of amendment and deletion are themselves capable of being amended or deleted, and if so, by whom.

70. I have begun enquiries with an individual with knowledge of the technical capabilities and access rights of the NSBIS database. I have not been able to complete these in time for response of rule 9-13. I intend to provide the answer to this paragraph as soon as possible.

Rule 9-13 paragraph 7:

With reference to paragraphs 37 and 58 – please confirm that neither of the two members of staff with access to the Legacy database have ever been the subject of allegations of inappropriate destruction or deletion of material. Please also confirm what if any steps have been taken to verify that there no conflicts of interest in respect of these two members of staff in relation to the subject matter of this Inquiry.

71. I have begun enquiries on rule 9-13 paragraph 7 and paragraphs 37 and 58 of my statement, but regretfully I have not been able to complete these in time for response of rule 9-13. I intend to update this statement in respect of the above as soon as possible and when enquiries are complete.

Rule 9-13 paragraph 8:

With reference to paragraph 60 – please explain what the “HMIC-approved RRD policy” says about what information may or should be routinely deleted from the current NSBIS database, and by what process (you may wish to provide relevant extracts from the policy). Please clarify the meaning of the following phrase: “Any records routinely deleted in accordance with that policy that may (unbeknown to the NCTPOC) have resulted from undercover policy [sic]...”; in particular please clarify to what extent a member of the NCTPOC tasked with carrying out the deletion – routine or otherwise - of material on the

OFFICIAL

NSBIS database would be able to ascertain whether material being deleted was relevant to undercover policing.

72. The RRD policy referred to sets out the criteria for deletion of records. In short it is by reference to the statutory obligations on information management as the MoPI policy. I understand the policy has been sent to the UCPI (it is the same as that referred to at paragraph 64 above).
73. In relation to knowledge of whether material is relevant to undercover policing I give the following explanation. NCTPOC receives intelligence from police forces and partner agencies. This intelligence has gone through the process of 'grading' by the time it is received by NCTPOC. Grading refers to the process whereby the owner of the intelligence assesses and records reliability of intelligence, to whom it may be distributed and does so with the aim of protecting its source. Once grading is complete, the source is not identifiable.
74. Individuals in NCTPOC are not able to find out from the face of the document or from enquiries with originators whether material is from an undercover police source. This is to protect the source. However, the originator of the information will know whether information has been produced from an undercover policing source and will have details of the undercover operation leading to its production, if it was such an operation. I understand that these organisations are under a duty to preserve material that relates to the UCPI as well.
75. I do not consider that the NCTPOC is obliged to preserve all of its material. Because it is not possible to isolate material originating from undercover policing after it has been graded, preserving the material would mean stopping all RRD. I do not consider this is proportionate or justified, particularly as the originating forces are obliged to keep the material that they can identify as being related to undercover policing

OFFICIAL

and the obligations relating to retention of information that apply to the MPS.

Rule 9-13 paragraph 9:

At paragraph 15 it is asserted that, following the merger of the NPOIU and other organisations in 2010 (which led to the creation of the NDEU), the NDEU “did not have the capacity to conduct undercover policing operations”. What happened to any undercover officers who had deployed under the auspices of the NPOIU prior to the merger, at this point? In particular who, or what organisation(s), took responsibility for such officers’ deployments, and/or the operations on which they were deployed? Was there a policy in place to manage any such transfer? If so, please provide a copy to the Inquiry.

76. This is not something within my knowledge for the reasons set out at paragraph 79 below. At present I am aware of one individual who is likely to know but the terms of rule 9-13 prevent me from asking this individual. I understand the MPS is seeking to provide a response to this paragraph as soon as possible.

Rule 9-13 paragraph 10:

At paragraph 23 it is asserted that reports sent to the NDEDIU would be drafted in such a way that the NDEDIU would not know the source of the intelligence. Following on from that assertion, to what extent is the role carried out by the NDEDIU as described at paragraphs 25-26, in particular the provision of a “threat picture” for the police and Whitehall, and the coordination and facilitation of intelligence gathering, performed without any explicit knowledge of the impact or results of undercover policing?

77. The threat picture is produced by aggregating intelligence received on a subject, critically analysing it and producing an overall assessment of a threat taking into account numerous aspects of intelligence received.

OFFICIAL

78. Since the reports provided to the NDEDIU did not reveal the source of the intelligence (as they had been through the process of grading described at paragraph 73 above), it follows that all work undertaken by the NDEDIU was performed without any explicit knowledge of the impact or results of undercover policing.
79. I wish to provide the following information relating to my role, which may help to clarify some of my responses dated 20 September 2016. As stated at paragraph 5, I have been in post since February 2016. Since this time I have been Head of Intelligence at NCTPOC. My role is primarily to perform a strategic function in relation to domestic extremism and counter-terrorism for NCTPOC. I manage the domestic extremism threat for the United Kingdom. I also manage a co-ordination role on counter-terrorism policing for the NCTPOC. This involves engagement with various stakeholders. The day-to-day running of the NCTPOC is overseen at Detective Inspector level. Where the terms of rule 9-13 permit, I will seek further responses where I have been unable to respond partially or fully by speaking to individuals in these positions.

I was also asked to answer the following questions by email dated 15 September 2016 (from Piers Doggart – Solicitor to the UCPI):

1. *Who is responsible for backing up the NSBIS database on a weekly basis?*

80. I understand that the systems backs up automatically to a hard disk weekly and to tapes daily. I am making enquiries as to responsibility for the overall management of this automatic backup process.

2. *How and where is the backup copy stored?*

OFFICIAL

81. The weekly backup is stored in [REDACTED]
[REDACTED] This room has appropriate physical security and access controls. The daily backup tapes are held on site with an appropriate failsafe measure in place for disaster recovery.

3. *Who has access to the backup copy?*

82. Individuals with access to the cabinet are IT Administrators: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; and Rob Cox. Individuals with the ability to recover from the back up tapes are [REDACTED] and [REDACTED].

4. *For how long is each weekly backup retained? By this, we mean is one week's back-up overwritten by the next week's or otherwise deleted / destroyed or does MPS have a library of week by week back up copies?*

83. Currently each weekly back up is overwritten after four weeks as the disks are on a 4 weekly rotation. There is no library and I understand that it is common practice to overwrite a backup with a more recent one.

Additions dated 28 December 2016

I make the following additions, corrections and clarifications following the 25th rule 9 request to the MPS, referred to as 'rule 9-25' and after reading witness statements made by Jeffrey Lamprey and Rob Cox in response to rule 9-13 and the 18th rule 9 request made to the MPS, referred to as 'rule 9-18' and by Ken Neale in response to rule 9-25.

Updates, corrections and clarifications

84. Having read Jeffrey Lamprey's witness statement originally dated 3 November 2016, as amended on 19 December 2016 ('Mr Lamprey's

OFFICIAL

statement'), I wish to make the following updates, corrections and clarifications to my witness statement:

- a. With regard to sub-paragraph 34(iii) of my witness statement, the shared drives referred to are of the I.T. system used by the NDEDIU (as it was then known) rather than the NSBIS database itself, as stated at paragraph 33 of Mr Lamprey's statement.
- b. In relation to paragraph 36 of my witness statement, NCTPOC staff are able to create and amend entries on NSBIS and these actions will be auditable. However, only Management of Police Information ('MoPI') reviewers are able to place entries on the 'weed list' so that they are deleted. An NSBIS user may trigger a review by placing a record on the review list but only following the review can an entry be deleted. The process is as set out at paragraphs 19 (as amended at paragraphs 37-38) of Mr Lamprey's statement.
- c. In relation to paragraphs 36 and 60 of my statement, I am now aware that deletion of an entry on NSBIS will remove the record of it from the NSBIS audit log (the t_audit log). The only record of the deleted entry that would remain is in a record of searches (if it had been searched for) and in the FoI log in respect of Nominal entities as set out at paragraphs 22 and 35 of Mr Lamprey's statement.
- d. With regard to paragraph 80 above, I confirm that NCTPOC's backups are the responsibility of the NCTPOC NSBIS Administrator and refer to paragraph 31 of Mr Lamprey's statement and paragraph 19 of Rob Cox's witness statement dated 28 November 2016 ('Mr Cox's statement').

OFFICIAL

- e. In relation to paragraph 83 of my statement I refer to exhibit JL/161103/5 as referenced at paragraph 32 of Mr Lamprey's statement as setting out how long backups are required to be maintained. Backups taken weekly are stored for four weeks. Daily backups are stored for ten days.
85. With regard to paragraphs 37 and 58 above I refer to Ken Neale's witness statement dated 23 December 2016. I am now aware that the five individuals referred to in Mr Neale's statement have access to the Legacy database. With regard to paragraph 71 above and the question at paragraph 7 of rule 9-13, I confirm that none of these individuals has been subject of allegations of inappropriate destruction or deletion of material. The following steps have been taken to verify that there are no conflicts of interest with these individuals in relation to the UCPI:
- a. Each of the individuals has been required to complete a declaration of associations form in the format provided to members of the MPS Assistant Commissioner's Public Inquiry Team to ascertain if they have any potential conflicts of interest with the subject matter of the Inquiry;
 - b. Each of the individuals has undergone national security vetting to Developed Vetting level as well as holding the MPS's own Management Vetting clearance.
 - c. In addition, each individual has been asked to sign a confidentiality agreement and has been verbally reminded of the requirement not to delete information of potential relevance to the UCPI. This is to reinforce the requirement to retain relevant information and to ensure that relevant material is not lost.
86. I also wish to make the following updates to my statement:

OFFICIAL

- a. With regard to paragraphs 38-39 I am aware that Operation Elter (the investigation into the NPOIU led by Chief Constable Creedon) has taken responsibility for reviewing the documents in the safes referred to. I am informed that the process of assessing them for relevance has not been completed.
 - b. With regard to paragraphs 43, 48 and 50 above I am now aware that a significant amount of electronic and hard copy material has been obtained by Operation Elter that may contain further information of relevance to the NPOIU. I am not aware of the detail of this material and understand that Operation Elter is analysing the material. I am not aware of the provenance of this material.
 - c. With regard to paragraphs 60 and 75 the NCTPOC has agreed to suspend all RRD for the purpose of ensuring that any potentially relevant information is retained for the UCPI.
87. In relation to paragraph 61 above I have been unable to locate the 2012 RRD policy. I have made enquiries with the individuals whom I believe may have known where it is but I have been unable to locate it. Regrettably, I am therefore unable to answer the request at paragraph 1 of rule 9-13.

Rule 9-18 paragraph 2:

Paragraph 66 (with reference to paragraph 60) – please clarify whether NPOIU records have or may have been routinely deleted from either the Legacy (as it is now known) or new NSBIS databases during each of the following time-periods:

- i. 2006-2010;*
- ii. 2010-2014 (up to the point of transfer of records to the new NSBIS database);*

OFFICIAL

- iii. *Since the transfer of records to the new NSBIS database in 2014;*

And if so, according to what criteria (or policy).

Please ensure it is clear from your response which database(s) you are asserting NPOIU records were or may have been deleted from, and whether those records can be expected to be present on the second database (if deletion occurred (or may have occurred) on only one of the two) and/or elsewhere.

88. I am unaware from personal experience or from speaking to individuals of the position in relation to the time period 2006-2010. However, I note that page 32 of the 2012 HMIC inspection referenced at footnote 1 of paragraph 32 above states:

"During the early part of the 2000s, a weeding policy was developed which meant a record would be removed from the database if there had been no new intelligence for six months. However, this never formed a definitive policy; and in practice, by 2006 weeding was not robust. The current database has an automatic weeding process, although it still requires human confirmation. Since 2008 more than 2,900 expired entries and documents have been removed from the database."

89. I note from this that HMIC concluded that expired entries had been deleted in the period from 2008 to the time of the report in 2012. All such entries deleted before the merger described at paragraph 13 above in 2010 would have been NPOIU records; a significant proportion of entries deleted after 2010 would also have been created by the NPOIU. Some of these records will have contained information that arose from undercover policing operations though I have no way of ascertaining what proportion did so. Any records deleted in this time period would not be replicated on the current, live NSBIS database.

OFFICIAL

90. For the period 2010-2014, the records on the NSBIS database used by the successor units to the NPOIU would have constituted partly of NPOIU records and partly of new records created by the successor units.
91. Any RRD that took place between 2010 and 2014 is likely therefore to have deleted NPOIU records in part. As stated at paragraph 32 above a significant number of records were deleted from 2012 to 2014 following the inspection by HMIC in 2012. These are extremely likely to have consisted partly of NPOIU records though I do not know what proportion of records deleted originated from the NPOIU in comparison to those created by successor units.
92. I note that paragraph 10 of Mr Cox's statement states that the review list for records on the NSBIS database became so large that it became locked and it was not possible to undertake RRD. Exhibit RC/281116/1 (dated 25 October 2013) states at page 2 that "*Currently the NDEDIU are not able to access the review list held on NSBIS. This is due to the volume of records and entities that are triggered or scheduled for review...*". This is consistent with my understanding from speaking to colleagues which is that RRD on the NSBIS database became impossible, leading to the creation of the 2014 instance of NSBIS.
93. From the above, my understanding is that some NPOIU records will have been deleted in the period 2010-2014 from what is now known as the Legacy database, though for a period of time no RRD was possible.
94. Any record deleted from what is now known as the Legacy database during this time will not be present on the new, live NSBIS database. For deleted nominal records, limited information will be present on the Legacy and new, live NSBIS database in the FoI log.

OFFICIAL

95. For the time period 2014 – present, RRD had been taking place on the live NSBIS database until it was suspended in October 2016. During this time, the live NSBIS database would have constituted partly of records created by the NPOIU and partly of new records created by the successor units (including NCTPOC). In the period that RRD had been taking place, some of the records deleted as part of RRD from the live NSBIS database would have been NPOIU records.
96. As all of the records on the live database at its creation came from what is now known as the Legacy database, any record disposed of as part of RRD from the new, live NSBIS database that had been created before the creation of the new database in 2014 would be retained on the Legacy database. Any record disposed of as part of RRD on the live database that had been created after creation of the new instance of NSBIS would not be on the Legacy database.
97. I do not know what proportion of the records deleted as part of RRD on the live instance of NSBIS is replicated on the Legacy database. However, as the time period from creation of the new instance of NSBIS in 2014 and the suspension of RRD is shorter than the SRD of many entities, I believe it is likely that most of the records disposed of during RRD would be older records (created before 2014) and retained on the Legacy database.
98. No RRD has taken place on the Legacy database in the time period 2014 – present.

Rule 9-18 paragraph 3:

Paragraphs 67 to 68 – the Inquiry understands paragraph 67 to assert that NCTPOC has no method of ascertaining whether information provided to it (and/or its predecessors) after 2014 relates to undercover policing; please clarify whether this is also the case for information provided to NCTPOC

OFFICIAL

(and/or its predecessors) in 2014, and before 2014. If the position was different in 2014 and earlier, please provide the date from which NCTPOC (and/or its predecessors) has been unable to identify whether information being provided to it is related to undercover policing.

99. The NCTPOC (and its predecessors) has no way of telling whether information provided to it in 2014 and before 2014 relates to undercover policing.
100. During the period when the NPOIU ran its own undercover operations, the part of the NPOIU that ran the operations would have knowledge that the information that resulted from the operation was from an undercover source.

Rule 9-25

101. I respond to the parts of rule 9-25 within my knowledge. In relation to sub-paragraph 6(1) I am aware that NCTPOC distributes threat assessments and/or intelligence requirements and forces will be expected to send information relevant to such assessments or requirements. However, I believe the policy, guidance or criteria used by forces to decide whether to send information to NCTPOC is a matter with forces' own knowledge and is not within my knowledge.
102. In relation to sub-paragraph 6(2) of rule 9-25 NCTPOC uses guidance provided by the College of Policing in the national standards of Intelligence Management and MoPI to guide whether to input information, and in what format, onto NSBIS.
103. NCTPOC staff members are expected to work in accordance with the principles of Intelligence Management as a whole but paragraph 2.3 of the *Intelligence report* section of Intelligence Management states:

OFFICIAL

Information content

...Information should be for a policing purpose. It should be clear, concise and without abbreviations. The information must be of value and understood without the need to refer to other information sources.

The body of the report should give no indication of the nature of the source, whether human or technical, or the proximity of the source to the information.

104. Information recorded on NSBIS is expected to comply with these requirements.
105. Further, paragraph 3.3.1 of MoPI states,

“Principles

There are key principles which apply, regardless of the format and business area where police information is held. The person recording the information must ensure that they have regard to these principles:

- a record must have been created for a policing purpose*
- all records must comply with the data quality principles*
- a record of police information is the start of an audit trail and must identify who completed the record, when it was completed and for what purpose*
- before recording information, checks should be made in other business areas to see whether the information is already held, thereby avoiding unnecessary duplication*
- if information is recorded on an individual who is the subject of an existing record, the record should reflect this*
- if it becomes apparent that the information being recorded is connected to other information, it must be appropriately linked*
- police information must be recorded as soon as is practicable in accordance with the standards relating to the business area in which the information is held*

OFFICIAL

- *consideration should be given to applying the appropriate government protective marking where appropriate, the source of the information should be recorded to ensure accuracy and to assist in requesting further information.”*
106. In relation to paragraph 6(3) I understand that secure emails sent to NCTPOC are kept on the system for one year, after which point they are reviewed. If the information is deemed to be of relevance, it is inputted onto NSBIS and the email deleted; if the information is not relevant, the email is deleted.
107. In relation to paragraph 11 of rule 9-25, as far as it relates to shared folders contained on the computer systems used by the NPOIU I believe that Operation Elter will be aware of the latest information regarding shared drives or personal folders used by the NPOIU. I believe that Operation Elter has a number of electronic storage devices used by the NPOIU. NCTPOC does not have a role in reviewing or storing this.
108. As far as the request relates to current usage of shared drives, I am aware that NCTPOC staff have been informed of the instruction to preserve information potentially relevant to the UCPI. The witness statement of Neil Hutchison dated 29 July in response to the 8th and 12th rule 9 requests sent to the MPS sets out the steps taken by the MPS in relation to this issue including engagement by Head of Information and Compliance of the National Counter Terrorism Policing Headquarters. This instruction has been to NCTPOC staff and has been reinforced verbally at management meetings. I do not have the dates of verbal reinforcement of instructions.
109. The likelihood that current personal folders on shared drives at NCTPOC contain information relevant to undercover policing is low, as the NCTPOC does not run undercover operations. However, I

OFFICIAL

understand that RRD on the NSBIS database has been suspended to ensure material of potential relevance is retained (even if NCTPOC staff are unaware of relevance without significant further information). I will review this issue for further steps that may be taken to ensure material of potential relevance is not deleted from shared drives currently in use.

110. In relation to the risk that staff or officers may deliberately seek to destroy or amend parts of the record and ensuring such attempts will be prevented or detected, I understand the record in this context to refer to the information on shared drives. Staff at NCTPOC are vetted to Security Check (SC) level. They are involved in collating and analysing information relevant to domestic extremism and counter terrorism threats to the UK and through this role they are made aware of the importance of maintaining honesty and integrity. The general factors impacting on conflicts of interest set out at Neil Hutchison's witness statement in response to rule 9-10(a) dated 9 June 2016 apply to staff and officers at NCTPOC, including police officer and staff discipline, the Police Code of Ethics and MPS values. The Department of Professional Standards also acts to ensure that deliberate dishonest conduct by officers or staff is prevented and detected. These factors reduce the risk that officers may seek deliberately to destroy relevant information.
111. In relation to paragraph 12 of rule 9-25, the concept of grading referred to at paragraphs 73-74 above is different to the concept of sanitisation (whereby 'unsanitised' information becomes 'sanitised'). Grading is the process described above whereby the owner of intelligence assesses and records the reliability of intelligence and to whom it may be distributed.
112. Sanitisation refers to the process whereby sensitive information is removed from the intelligence. A person grading intelligence may also

OFFICIAL

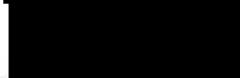
sanitise it, as the nature of information that remains will dictate to whom it may be distributed. For example, if a record contains details that reveal the information has originated from a CHIS, the owner may restrict distribution further than if that part of the information had been removed.

113. NCTPOC receives information after it has gone through the process of grading and after it has been sanitised to the extent that the identity of the source (including whether it is an undercover officer or a non-undercover officer CHIS) has been removed. However, it is possible to 'sanitise' information received by NCTPOC further, for example to remove personal details identifying witnesses, victims, intelligence vulnerabilities.

114. I understand the reference to unsanitised and sanitised information on NSBIS referred to at exhibit RC/281116/1 to refer to information that is stored as it is received from the originating force (which is referred to as unsanitised even though the identity of the source would already have been removed) and to a modified entry on NSBIS that may remove further details (referred to as sanitised, which may be to enable wider sharing).

I believe the facts stated in this witness statement are true

Signed.....

Dated..... 3.1 2017