Statement made on behalf of:	The Commissioner of Police of the Metropolis
Witness:	Rob Cox
Statement No:	2
Exhibits Referred to:	RC/281116/1
Date Statement Made:	4 January 2017

IN THE MATTER OF: PUBLIC INQUIRY INTO UNDERCOVER POLICING

Witness:	**Rob Cox**
Occupation:	Head of Information Assurance and Accreditation, NCTPHQ
Address:	c/o Directorate of Legal Services, 10 Lamb's Conduit Street, London, WC1N 3NR

I believe the facts stated in this witness statement are true

Signed [redacted]

Dated 04/01/2017

Preface

On 28 November 2016 I made a witness statement that consisted of 23 paragraphs. That statement read as follows:

Signature: _____ Date: _____

Introduction

1. I am the Head of Information Assurance and Accreditation for the National Counter Terrorism Policing Headquarters ("NCTPHQ").

2. I joined the Metropolitan Police Service ("MPS") in 2007 after working as an MPS student contractor within Digital Policing after studying computer science at university. I then worked for SO15 as an intelligence officer for two years. From 2009 – 2012 I was a project support officer for the London Olympic Intelligence project.

3. In late 2012, when coming to the end of the Olympic Intelligence project, I was asked by my Senior Management to assist the National Domestic Extremism Unit ("NDEU" as it was then known) to provide assistance with its Information Systems. In January 2013 I undertook the role of Information and Communications Technology ("ICT") Security Manager. This role was to provide technical and security assistance and advice to the unit. I continued in this role until October 2015 when I left to become the Head of Accreditation at the National Counter Terrorism Policing Headquarters ("NCTPHQ").

4. I was initially asked by the NDEU to help stabilise its National Special Branch Intelligence System ("NSBIS") as the unit was experiencing some difficulties in its use. Following this, and after reports by Her Majesty's Inspectorate of Constabularies, I was tasked by the Senior Leadership Team ("SLT") to improve the way that records were managed on NSBIS so retention, review and disposal ("RRD") of records could be applied in accordance with the type of information held in records and in particular their relevance to different areas of policing, such as public order, domestic extremism, extreme left wing, extreme right wing etc.

Signature: _____ Date: _____

5. The way that the NDEU (by then known as the National Domestic Extremism and Disorder Intelligence Unit ("NDEDIU")) decided to achieve this was to create a new instance of NSBIS in 2014. I provided technical assistance to implement this change with Detective Chief Inspector [redacted] having overall responsibility. The design and implementation process was agreed with the accreditor, Jeff Lamprey of the Association of Chief Police Officers Terrorism and Allied Matters Information Security Services.

6. My experience as detailed above means that I have knowledge of changes and developments in the NSBIS system of the NDEU (and successor units), in particular over the period 2013 – 2015.

7. I am aware that the Undercover Policing Inquiry ("UCPI") has requested information from the MPS about NSBIS and related matters. I have read a witness statement given by Temporary Detective Superintendent ("T/DSupt") Michael Killeen (dated 22 June 2016, amended 20 September 2016) in response to the UCPI's rule 9 requests referred to as rule 9-10(b) and rule 9-13 as well as responding to questions sent by email dated 29th September 2016. I am also aware of an additional request referred to as rule 9-18.

8. The remainder of my witness statement is organised as follows: firstly, I respond to outstanding aspects of the rule 9-13 request that are within my knowledge; secondly, I will provide responses to questions asked by email that are within my knowledge; thirdly, I will address aspects of rule 9-18 within my knowledge.

Rule 9-13

9. I will refer to the UCPI's request by the numbered paragraphs of the rule 9-13 request.

Signature: _____ _____ Date: _____

Paragraph 1

10. With regard to paragraph 1, I did not apply the criteria set out in the 2012 RRD policy as that was an operational matter. My role was to assist with technical / functionality aspects of RRD. In this respect, I recall that at some point in the period 2012-2013 the review list became locked because it was too large and I believe that during the period that the review list was locked it was not possible to undertake RRD.

Paragraph 2

11. In relation to paragraph 2, I was not asked to check whether records had been deleted from the Legacy database since 2014. I am aware that access to the physical location of the Legacy database was restricted and access to the database was restricted to a small number of user log ins.

12. As the Legacy database still exists, a forensic examination of that database and the live NSBIS database may be possible to compare differences between the two, but this is not certain. This is because there are a number of factors that could determine if information is recoverable and comparable. This could include, for example, the time spent to compare the files, how the two systems are configured and if the files have been overwritten or amended on the hard drive by the operating system.

13. I am also aware that the relevant parts of the document setting out the business case for the new instance of NSBIS (the document is dated 25 October 2013 and the relevant pages to this request are set out at Exhibit RC/281116/1) state:

"*A number of NSBIS terminals will be made available for staff to search the old system. This will be limited to specific roles outlined below since all*

privatised documents will now be visible. User access rights within the old instance of NSBIS will be set to read only using SB House so no data can then be added to it and all new intelligence being added via the SPOE [single point of entry] will only be added to the new system…

Risk Management…

Risk of all staff being able to view sensitive intelligence held on old system.

This risk is minimised by a number of practices. All staff within the unit hold a minimum of SC vetting and will be [redacted] *inducted. There will be a limited number of desktops allocated to view the old system. Reports will be generated weekly to audit staff who have accessed the old system. This will be undertaken by the Local IT and Security Manager…*

Risk of data loss or corruption of new system

There will be limited risk since the new system will be located on a new server. The old server will run and will have a back up tape. The new server will have its own backup tapes which would follow the current process for business continuity (i.e. one tape off site and the other daily tapes located on site, with additional terra station for weekly back ups).."

Paragraph 3

14. In relation to paragraph 3, as stated above I was not involved in selecting the records to be transferred from the Legacy to the new, 2014 NSBIS instance as these were operational decisions. However, I am aware that the relevant parts of the document setting out the business case for the new instance of NSBIS (as at Exhibit RC/281116/1) state:

Signature: _____ Date: _____

"All the NDEDIU nominal have recently undergone a rigorous intelligence review as part of HMIC recommendations. Nominals that did not meet the threshold were weeded as part of this review with the existing nominals subject to ongoing reviews as part of the review, retention and disposal management."

Paragraph 5

15. In relation to paragraph 5 I believe that although the term NSBIS refers to the intelligence database, it was also used to refer to the computer network in operation at NDEDIU (and successor units). The shared drives referred to at paragraph 5 of rule 9-13 appears to be to the shared drives on the computer system, as the actual NSBIS database did not have shared drives.

16. Individual users may have worked on files saved on their personal drives or on shared drives before uploading intelligence records to NSBIS so it is possible that information that is not on NSBIS relevant to the UCPI was contained on shared or personal drives.

17. Access to the NSBIS audit log and the NSBIS FoI log is controlled by the local NSBIS Administrator.

Emailed questions

18. This section refers to the questions mentioned at paragraphs 80 – 83 of T/DSupt Killeen's witness statement.

19. With regard to question 1, during my time serving in the NDEU and successor units, I was responsible for backups. On leaving the unit, I trained two individuals, [redacted] and [redacted], to undertake backups but I am not

Signature: _____ Date: _____

aware of who is responsible for them at the present time. Weekly backups were conducted automatically. Daily backups required manual insertion of tapes.

20. In relation to question 2, the daily backup was stored in a fire proof container within a secure cabinet, on site. Weekly backups were written to a local storage device. One back up tape was stored off site. The Legacy database is stored on local servers and infrastructure, within a secure Technical Equipment Room at [redacted]

21. In relation to question 3, on 03/11/2016 I was advised that from the Access Control System the following staff previously had physical access to the Technical Equipment Room (TER), [redacted], [redacted], [redacted] and [redacted]. I was later advised that these were removed and replaced with [redacted], [redacted], [redacted], [redacted] and [redacted]. While I was in post I believe only myself and [redacted] had access to the TER.

Rule 9-18

22. In relation to question 1, only some of the records contained on what became the Legacy database were transferred. As to the selection and transfer of records I refer to my response to paragraph 3 of rule 9-13 above.

23. In relation to question 2 I am only aware of the situation from when I joined in 2012/2013. As stated above I am aware that the review list was locked at some point prior so no RRD was possible. When the new instance was created, RRD was enabled.

I now wish to update my statement as follows.

Signature: _____ Date: _____

Update dated 28 December 2016

24. Correction to paragraph 19 above: the name [redacted] should read [redacted]

25. Correction to paragraph 21 above: the name [redacted] should read [redacted]'.

26. In relation to sub-paragraph 10(1) of the 25th rule 9 request made of the MPS ('rule 9-25'), I believe the definitions of security groups contained at exhibit RC/281116/1 remained the same when the new instance of NSBIS was created in 2014. I have noted that page 4 of exhibit RC/281116/1 states that the Protest and Disorder security group had the code "PR". I am now aware that the code for the Protest and Disorder group was "PT". I believe that exhibit RC/281116/1 notes the code incorrectly at page 4 (in that it should read "PT Security group" at the second bold sub-heading) but the definition remained in use for migration to the new NSBIS database.

27. I also note that exhibit JL/161103/2 of Jeff Lamprey's witness statement dated 3 November 2016 refers to "PT (Protect)". I believe this is an error in the description of the "PT" coded security group which should read "Protest" or "Protest and Disorder" instead of "Protect".

28. In relation to sub-paragraph 10(2) of rule 9-25 I do not believe that written definitions of NSBIS security groups existed at the NDEDIU (or predecessor units) prior to the creation of the new instance of NSBIS in 2014.

Signature: _____ Date: _____