Statement made on behalf of:	The Commissioner of Police of the Metropolis
Witness:	Neil Hutchison
Statement No:	1
Exhibits Referred to:	
Date Statement Made:	17 June 2016

IN THE MATTER OF: PUBLIC INQUIRY INTO UNDERCOVER POLICING

Witness:	Neil Hutchison
Occupation:	Police Officer
Address:	

I believe the facts stated in this witness statement are true

Signed...[redacted].................

Amendments to statements:

I provide this statement in response to a request for clarification/further information from the Undercover Policing Inquiry (UCPI) dated 1 July 2016 to the witness statement in response to the eighth rule 9 request of the MPS dated 15th January 2016. That witness statement was first provided on 29 January 2016, extending to 56 paragraphs. An update was provided on 3 June 2016 extending the statement to 72 paragraphs and a further update provided on 17 June 2016 extending the statement to 87 paragraphs. This statement read as follows:

Rule 9-12

Signed: [redacted] **Date:** 29th July 2016

I provide this statement in response to the twelfth Rule 9 request which asks for clarifications in relation to the statement provided in response to the eighth Rule 9 statement. That response to the eighth Rule 9 statement was first provided on 29 January, extending to 56 paragraphs. An update was provided on 3 June 2016 extending the statement to 72 paragraphs. That statement read as follows:
On 29 January 2016 I made a statement of 56 paragraphs. This statement was updated and extended to 72 paragraphs on 3rd June 2016. This statement read as follows:

I make this statement as an addition to my previous statement to the Undercover Policing Inquiry dated 26th January 2016 submitted in response to Rule 9 (8) dated 15th January 2016. I submit this additional statement in order to provide updates to some of the information supplied in my previous statement and to provide clarification in relation to some issues covered in that statement.

Introduction

1. I am a Detective Superintendent in the Metropolitan Police Service, currently fulfilling the role of Police Team Senior Officer (PTSO) for the Assistant Commissioner Directorate of Professionalism's Public Inquiry Team (AC-PIT). At present my line manager is Deputy Assistant Commissioner Fiona Taylor who is responsible for the Directorate of Professional Standards in the Metropolitan Police Service (MPS).

2. I make this statement in response to the Undercover Policing Inquiry's (UCPI) eighth Rule 9 request to the MPS dated 15th January 2016 and in particular to the request for "...a witness statement setting out the steps taken by the MPS to preserve information which may be of relevance to the Inquiry, and to prevent potentially relevant documents from being lost or destroyed." The UCPI has asked that the response include, without limitation:

Signed: [redacted] Date: 29th July 2016

"(1) Details of all requests or instructions by you to your staff to preserve MPS documents for the purposes of this inquiry;

(2) Any steps that have been taken to verify that any request or instruction to preserve documents is being complied with;

(3) The steps that have been taken to address the risk that individual officers or staff may deliberately seek to destroy or amend parts of the record, and to ensure that any such attempt will be prevented or detected;

(4) Details of any instance in which you suspect that any officer has circumvented, or sought to circumvent, the steps taken;

(5) The ways in which routine or automated document destruction procedures have been modified to ensure that relevant documents will not be destroyed."

3. In preparing this statement, I have had regard to the provisions of the draft Disclosure Protocol between the MPS and the Inquiry:

"Aims
4. (e) that all appropriate steps to prevent potentially relevant documents in the possession of the MPS from being lost or destroyed are taken;
[...]

Preservation of information by MPS
6. The MPS will take all reasonably practicable steps to preserve all information which may be of relevance to the Inquiry. It will keep the Inquiry team informed as to the steps which it takes in order to do so.
[...]

Retention of documents

Signed: [redacted] **Date:** 29th July 2016

30. The MPS should ensure that it retains original versions of all documents and physical evidence relevant to the Inquiry and that relevant information is not destroyed."

Qualifications and experience

4. My current role and recent experience enables me to provide the statement requested by the UCPI.

5. I was posted into HQ Professional Standards in May 2014 to join a team then known as Operation Beacon. The Op Beacon team was a newly developed unit engaged in responding to a range of work emanating from the findings of the Stephen Lawrence Independent Review (SLIR) conducted by Mark Ellison QC, the findings of Operation Herne and an announcement by the Home Secretary that a Public Inquiry would take place into undercover policing. From May 2014 to June 2015 the team was led by Detective Chief Superintendent Jeremy Burton although from December 2014 to March 2015 DCS Burton was attending the Senior Police National Assessment Centre (PNAC) course.

6. My work since May 2014 has involved a number of roles and responsibilities in relation to the following Strategic Objectives for Op Beacon established by MPS Management Board on 16 April 2014:

(i) To support the work of Mark Ellison QC on the review of specific cases;
(ii) To support the Public Inquiry;
(iii) To support the [redacted]PCC corruption investigation;
(iv) To support the work of Operation Herne;
(v) To review the issue of document handling and the MPS approach to records management;
(vi) To demonstrate transparency throughout; and,
(vii) To learn any lessons on undercover policing, implement changes and embed organisational learning.

Signed: [redacted] **Date:** 29th July 2016

7. From January 2015 I took over leadership of the Op Beacon team. In that role I was responsible for all the Strategic objectives described in para 6. In relation to objective (v) Operation FileSafe was commenced in May 2014. The purpose of Op FileSafe is to review MPS document handling and record management and complete a thorough assessment of all physical records held across the MPS estate. Significantly for the purposes of this statement, Op FileSafe is the mechanism by which instructions to retain documents potentially relevant to the UCPI have been disseminated throughout the MPS. Op FileSafe is one of several roles undertaken by the Op Beacon team. In June 2014 the Op Beacon team was re-designated as the Assistant Commissioner's Public Inquiry team (AC-PIT). On 20th July 2015 Superintendent Parm Sandhu joined the team and took over responsibility for the review of anti-corruption operations and support of [redacted]IPCC investigations which enabled me to work full time on the upcoming UCPI and delivery of Operation FileSafe. From September 2015 officers and staff were assigned to provide dedicated support to the UCPI. I then split the AC-PIT team into Strand 1, which is dedicated to the UCPI and Strand 2 which is dedicated to review and disclosure of anti-corruption material.

8. I have worked closely with the MPS Records Management (RM) and Information Assurance and Security leads in delivering Op FileSafe. I have sought independent advice on Information management by approaching the National Archives at Kew. I subsequently appointed an expert in Information management from a public sector organisation dealing with sensitive material to the Independent Scrutiny panel that provides advice to AC Hewitt and myself. Officers deployed on Op Beacon have developed extensive experience of providing disclosure to reviews and investigations addressing legacy issues; including Mark Ellison QC's SLIR, [redacted] two IPCC investigations, the Daniel Morgan independent panel and an MPS review of anti-corruption investigations since 1994.

Signed: [redacted] Date: 29th July 2016

Structure of statement

9. I have addressed the issues raised by the eighth Rule 9 request under the following headings:

(i) The risk of potentially relevant documents being lost or destroyed;
(ii) General approach to retention of data relevant to the UCPI;
(iii) Operation FileSafe; and,
(iv) The five specific issues raised by the UCPI.
Appendix 1: Timeline of delivery of Op FileSafe
Appendix 2:Operation FileSafe progress report to December 2015

The risk of potentially relevant documents being lost or destroyed

10. I have been conscious throughout my involvement of the importance of retaining material relevant to the UCPI's terms of reference (ToR). Throughout my work with Op Beacon and Op FileSafe I have identified several risks to the full retention of potentially relevant documents to the UCPI terms of reference and I have taken measures detailed in this statement to minimise their impact.

11. The first identified risk to the retention of potentially relevant documents is the failure to identify those documents. The primary reason for this risk is the complexity and number of information management systems operated by the MPS and the changes to those systems throughout the period under review by the UCPI, in particular the transition from paper based to IT based systems. The level of complexity of MPS systems and processes is a reflection of the wide range of roles and responsibilities of the MPS. The MPS uses several hundred different IT systems and a range of different document archive systems. There is no central and standardised Information Asset Register (IAR). Op FileSafe has commissioned development of an IAR but to

date this has not been achieved. At present the MPS Record Management System (RMS) is being used as an interim solution to record material located during Op FileSafe reviews of local and deep storage document archives. AC-PIT have scoped MPS IT based Information management systems that hold material potentially relevant to the UCPI and have found their search capabilities to be highly variable with some having no effective search capability at all. A further complication is that a number of databases have been through several migration processes and upgrades over their lifetimes. The search capability may therefore vary depending on the time period relevant to the search. The MPS requirement to maintain operational security leads to material being held in isolated systems with restricted access or within tiered security access.

12. Intentional destruction of relevant material is a second risk that I have considered, and measures to control this risk are described in this statement. I am acutely conscious of the damage that can be caused to public confidence in policing by the suggestion that material has been purposefully or inadvertently lost or destroyed.

13. Disposal of material can take place for numerous reasons and there has been a lack of standardised systems to record what has been destroyed and why. Operation FileSafe is addressing this is relation to document archives through recording reviewed material on the MPS Record Management System (RMS) and implementing a standardised Retention, Review and Disposal (RRD) process. There are extensive programmes underway in the MPS to reduce the number of vulnerable non-corporate IT systems in use and reduce use of paper records by implementing digital working. These are addressing current Information management risk but are very long term programmes which are unlikely to resolve current challenges to providing full disclosure to the UCPI.

14. The MPS does not use automated destruction procedures for documentary material as this would be incompatible with the need to assess whether there is an ongoing policing requirement to retain the material. Management of

Signed: [redacted] **Date:** 29th July 2016

Police Information (MoPI) principles and the Data Protection Act 1998 require the MPS to review a wide range of categories of material held prior to destruction. The UCPI are referred to College of Policing (CoP) Authorised Professional Practice (APP) on Information management for detailed guidance on implementing MoPI. The CoP APP is available on line (https://www.app.college.police.uk/app-content/informationmanagement/management-of-police-information).

The key points in relation to decision making on destruction of material are outlined in the National retention assessment criteria described in the CoP APP (D785). It follows that a large proportion of material is retained for longer than the minimum periods determined by its MoPI review group. Any request for material therefore requires considerable research in order to:

(i) Identify where it should be held or might be held;

(ii) Determine whether it is likely to still be held or may have been destroyed under MoPI or previous policies;

(iii) Research what information management systems are in use by the various holding units and who can access them;

(iv) Set appropriate search parameters and task searches to staff with access to and understanding of the specific information management systems;

(v) Once located to review the material to determine whether it is complete or further enquiries are required;

(vi) If the material is not immediately located to review what, if any, systems are in place for recording destruction or transfer of the material and arrange research of those. When the material is historic it is important to recall that current Information management systems may not include back record conversion of material from before the system was implemented due to the prohibitive scale of material held; and,

(vii) If the material still cannot be located to consider steps that can be taken to locate it.

Signed: [redacted] Date: 29th July 2016

General approach to retention of data relevant to the UCPI

15. On receipt of a Rule 9 disclosure requirement from the UCPI the following steps are taken to identify and secure the relevant documents for disclosure.

Step 1 – MPS Directorate of Legal Services (DLS) copy the Rule 9 to AC-PIT as soon as it is received.

Step 2 – MPS DLS analyse the request and prepare a schedule for AC-PIT to provide broad guidance on the material which could be relevant to each element of the Rule 9.

Step 3 – AC-PIT consider what and where material may be held. AC-PIT raise Actions on the Holmes case management system and assign them to officers to commence enquiries to locate the material.

Step 4 – Where relevant material can be accessed by AC-PIT staff, for example material held on the Op Herne Holmes account, AC-PIT staff will conduct their own searches and copy the located material across to the AC-PIT Holmes account from where it will be scheduled and prepared for disclosure to DLS. Where appropriate written search parameters are provided directing systems, search terms and time parameters for searches. These are linked to the Action on Holmes.

Step 5 – Where relevant material is held, or believed to be held, by units who retain the material on secure IT systems AC-PIT will engage with appropriate staff on those units to arrange access. This process has been relevant to Rule 9(4) and Rule 9(7). Initial engagement is usually at Superintendent/Detective Chief Inspector level. Engagement makes clear the legal obligations under the Inquiries Act 2005 to comply.

Step 6 – AC-PIT conduct engagement with relevant units to identify what relevant material may be held and provide the unit with a schedule or other written directive describing the material required and expectations on the unit to research and provide it. The schedule used for Rule 9(4) contained a further written reminder of the legal obligation to provide the material. The unit work through the schedule to identify and provide relevant material. AC-PIT have, where appropriate, assigned officers to work with units in reviewing their databases and identifying relevant material.

Signed: [redacted] Date: 29th July 2016

Step 7 – On receipt of material AC-PIT review it and compare it against AC-PIT and DLS schedules to ensure the material for disclosure meets the UCPI's requirement. AC-PIT assess at this stage if further enquiries are required and if the material provided to date identifies further material or sources of material which may be relevant.

Step 8 – AC-PIT provide the material and updated schedule to DLS who conduct a further review of material and, if necessary, provide follow up enquiries for AC-PIT to undertake or directions for briefing notes to assist the UCPI's understanding of the material.

16. Activity in preparation for the UCPI has focused on developing an understanding of what material could be considered relevant to broad terms of reference, scoping where such material may be held, how it could be recovered and developing a case management system capable of coping with disclosure of highly sensitive material on a unprecedented scale.

17. While the Inquiry ToR was not established until July 2015 my approach since my deployment to Op Beacon in 2014 has been to consider any material linked to the deployment of undercover officers as potentially relevant to the UCPI. Preliminary instructions e mailed to Basic Operational Command Unit (BOCU) Commanders on 29.07.14 and 01.08.14 stated "7. At present there is no MOPI period for retaining material relating to police corruption investigations or undercover operations. Please ensure that if any such material is found it is retained and e mail DPS - AC Public Inquiry Team with details."

18. I also considered, from an early stage, how to ensure such potentially relevant material would be retained. My initial considerations were as follows:

(i) The terms of reference for the Inquiry were not known;

(ii) Operation Herne had secured relevant material to the operations of the Special Demonstration Squad (SDS). This material was held in a

Signed: [redacted] Date: 29th July 2016

secure environment with access restricted to officers attached to that investigation;

(iii) Material relevant to the operations of the National Public Order Intelligence Unit (NPOIU) 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;

(iv) Undercover policing is not a defined category of material under MoPI or in the MPS Records Management System (RMS). The subject matter is a tactic potentially relevant to a wide range of units, operations, investigations and policy areas. Material potentially relevant to the Inquiry would not be located in a clearly defined area nor was it possible to search for such material on Information management systems. A search for 'undercover operations' on RMS or local archive systems would not provide a meaningful result; and,

(v) Records of undercover deployments held in SC&O35 could be cross-referenced to identify relevant case files. However, given the number of such operations conducted by the MPS I did not consider it proportionate to identify and recover all material relevant to these operations. It would be an extremely resource intensive task to recover material most of which is unlikely to be required by the Inquiry. A further consideration relating to this decision was that the record of operations commences around 2000. Under current MPS policy files relevant to investigations where undercover officers were deployed are likely to attract a retention period of at least 12 years and in many cases 30 years.

19. In terms of addressing the storage of potentially relevant material on numerous information management systems, my general position has been to retain potentially relevant material in whichever information system or archive it is currently stored until such time as it becomes relevant to a Rule 9 request from the Inquiry, at which point it can be retrieved. I considered this a proportionate response to the need to retain potentially relevant documents

Signed: [redacted] Date: 29th July 2016

across numerous information management systems pending the development of an UCPI-specific document management system. As is detailed below, it would not be possible to collate all of the material in an existing central system.

20. In relation to the possibility that paper documents relevant to the UCPI could be destroyed through routine review and disposal procedures the key factor is that the MPS do not operate any automatic destruction process. All material held on MPS systems is subject to review prior to destruction to determine if its retention is required. In relation to paper material there is no auto-deletion or destruction of any material from the General Registry. There is an ongoing 'call-back' process by which files which may have reached their review period are called back from storage for review by General Registry staff. General Registry have been fully engaged with Op FileSafe, the staff who conduct reviews are aware of the need to retain and inform AC-PIT of any material reviewed for destruction which appears relevant to undercover operations. There is, and has not been in the past, any policy of 'unreviewed destruction / deletion' from the MPS General Registry. This applies to material held either at Hendon Repository or the deep-storage facility. Staff at the deep storage facility do not undertake any review or destruction of the MPS material. Material held in local archives, sometimes known as 'File on Division' is subject to review for destruction by BOCU staff with responsibility for managing the local archive. Under Op FileSafe a review was undertaken of MPS Records Management Policy and instructions. A new Records Management toolkit was disseminated across the MPS in early 2015 which makes clear the requirement on all staff to review material prior to destruction (D760, D774). The toolkit review process map makes specific reference to retaining any material reviewed relevant to undercover operations and provides a proforma to flag such material to AC-PIT for consideration.

21. In relation to digitally held material potentially relevant to the UCPI there is only one corporate database currently used by the MPS with an integrated auto-delete function. This system is NSPIS (National Strategy for Police

Signed: [redacted] Date: 29th July 2016

Information Services - http://www.met.police.uk/foi/glossary.htm). NSPIS is a national system over which the MPS has limited control or direction. NSPIS is primarily used for generated and management of custody records and criminal justice case files. The creation of an NSPIS record generates footprints in other systems (such as PNC or Cris), meaning that after the details of the period in custody have been deleted, the trace of that record remains within other systems dependent on the nature and outcome of the period of detention. Applications can be made for deletion of a PNC record, however there is no auto-delete on this key national database. Dependent on the nature of the arrest and outcome a copy of the custody record is likely to be retained elsewhere within the crime file. For instance, in a homicide investigation, the NSPIS record would be recorded and retained with the HOLMES account and the General Registry file.

22. The duplication of computer records within General Registry files and other recording systems is a key consideration in relation to ensuring retention of relevant material for the UCPI. The processes involved in running undercover operations involve the recording of material across a range of systems. Relevant material held on a corporate database subject to destruction review, such as Crimint, will be a disseminated and sanitised version of the original intelligence report held in the originating unit's operation file. Such operation files are stored in GR and recorded on the Records Management System (RMS). The work of Op FileSafe to review locally held files is therefore key to identifying, filing and recording any such operational files which have not been submitted to GR or have been otherwise misplaced or incorrectly filed.

23. I consider that suspension of all MPS review and destruction processes for the duration of the UCPI would be disproportionate given that:

(i) The vast majority of material held by the MPS is not relevant to the Inquiry;

(ii) The MPS is legally obliged to review and dispose of material to comply with MoPI and data protection legislation;

Signed: [redacted] Date: 29th July 2016

(iii) A suspension of normal destruction procedures for several years would create a massive backlog of material for disposal;

(iv) The current use of real estate for archiving documents is an inefficient use of space;

(v) The MPS corporate real estate programme involves disposal of the majority of real estate controlled by the MPS. In order to achieve that programme, which is crucial to implementation of recent budget reductions, the MPS is required to destroy or relocate documentary archives held in real estate scheduled for disposal.

Operation FileSafe

24. A timeline of key decisions and milestones in relation to the delivery of Op FileSafe is provided at Appendix 1. In this statement I intend to provide an overview of a highly complex and ongoing operation to improve MPS Records management in relation to physical material, primarily paper files and locate misplaced or incorrectly filed material. The strategy for delivery of Op FileSafe has changed in response to information gathered in scoping, liaison and pilot work and in order to prioritise premises scheduled for disposal. In this section of my statement I intend to provide a general overview of activity directly relevant to the questions raised by the UCPI in Rule 9(8) and to cross-refer this overview to relevant documents. Further information and reference material regarding Op FileSafe can be provided to the UCPI if required.

25. Operation FileSafe was commenced in May 2014 in response to Mark Ellison QC's comments in the SLIR about the difficulties he experienced in locating relevant material due to weaknesses in MPS Information management. The purpose of Op FileSafe is to review MPS Record management of documents and material held on portable digital storage devices and to conduct a thorough assessment of all physical records held in offices and other premises across the MPS estate. The MPS Management board directed Operation Beacon to deliver Op FileSafe. I led on delivery of Op FileSafe as part of my Op Beacon responsibilities. There has never been any dedicated

Signed: [redacted] Date: 29th July 2016

resource for delivery of Op FileSafe but I have been assisted in planning and delivery of the Operation by one Detective Inspector assigned to Op Beacon on 1 September 2014. Delivery of Op FileSafe has been conducted by engagement with various units across the MPS to scope the current position in relation to Records management, develop a strategy and implement improvements to the management of physical records.

26. DAC Rodhouse proposed the following objectives for Op FileSafe on 20 May 2014:

To conduct a thorough assessment of all physical records held in offices and other premises across the MPS estate in order to understand:

(i) Do the MPS need to retain the material?
(ii) If so then is it appropriate to be held locally?
(iii) Is there adequate indexing of the locally held data and is there sufficient corporate knowledge of its content and presence?
(iv) Should the data be held in corporate archives?
(v) To assess opportunities to utilise scanning and automated indexing solutions to reduce the volume of material held in corporate archives.
(vi) To assess whether any material located as a result of Op FileSafe has relevance to any of the terms of reference for Operation Beacon.

27. Op Beacon subsequently developed a Terms of reference for Op FileSafe (D769) to:

(i) Review records management policy;
(ii) Obtain independent scrutiny;
(iii) Conduct an operational review to ensure integrity of documents held outside agreed storage;
(iv) Support delivery of Record management strategy and associated internal awareness campaign; and,

Signed: [redacted] Date: 29th July 2016

(v) Work with Total Technology programme to identify options for conversion of hard copy records into digital, searchable formats.

28. Successful delivery of Op FileSafe is required in order to achieve all Op Beacon strategic objectives including the objective to support the UCPI. In relation to the questions raised in Rule 9(8) I consider Op FileSafe to be highly significant to the UCPI as:

- Inappropriate storage and lack of searchable records of files held in local archives and deep storage are a key risk to the MPS' ability to provide full disclosure
- Delivery of Op FileSafe has, since 2014, been used to disseminate the message that material relevant to undercover policing must be retained for the UCPI.

29. I consider the review of material held in local archives and deep storage to be the key focus as organisational learning from the SLIR and Op Beacon's work has been that local and deep storage documentary archives are a very significant vulnerability in MPS information management. Scoping activity undertaken by Op FileSafe identified that a considerable quantity of material that should be submitted to General Registry, and recorded on RMS, is instead held in local archives. It was further identified that when material is recorded in RMS but cannot be located in General Registry the most likely explanation is that it has been recalled by an operational unit and then never returned to Registry. Such material is likely to still be held in local archives and office areas. Op FileSafe is the ongoing project to locate such incorrectly archived and stored material, dispose of it appropriately and standardise recording processes to improve the ability of the MPS to recover such material.

30. The development and delivery of Op FileSafe is a highly complex project involving extensive engagement across the MPS and consultation with members of an Independent Scrutiny panel appointed to advice AC Hewitt and myself. This panel includes a recognised expert on Information

Signed: [redacted] Date: 29th July 2016

management in government agencies [redacted] (D762). Op FileSafe is a very significant factor in MPS efforts to ensure appropriate disclosure to the Inquiry given the aim of addressing issues identified with MPS Records management with the potential to undermine successful disclosure to this and other Inquiries or investigations.

31. Op FileSafe relates to physical records defined as paper files and digital material held in portable forms such as memory sticks and CDs. Existing corporate IT systems are outside the scope of Op FileSafe. These are subject of a major long term change management programme under Total Technology to review and update systems to enhance storage and interaction capabilities. The overarching transformation project is called TTPi - Total Technology Programme Infrastructure.

32. In 2014/15 Op FileSafe engaged extensively with senior staff leading on Total Technology, Digital Policing and Information Law & Security. This engagement included raising awareness of the upcoming Inquiry and necessity to retain and recover relevant material. Work has been undertaken by AC-PIT to develop our understanding of the complex range of systems potentially relevant to the Inquiry and ensure that appropriate search parameters are set. In 2015 Op FileSafe identified the range of IT systems currently in use by the MPS and assessed those which may contain material relevant to the UCPI ToR. A number of these are key corporate systems such as Crimint. Managers responsible for key systems such as INFOS and IMOS have been engaged by Op FileSafe and the Public Inquiry team in relation to their systems and are aware of the requirement to retain material relevant to the UCPI.

33. During scoping and consultation work conducted throughout 2014 I identified a series of key risks to Information management of documentary archives. This led to my recommending a change of strategy for the delivery of Op FileSafe. My findings were delivered to AC Hewitt who, as Management board

Signed: [redacted] Date: 29th July 2016

lead, approves the strategic direction of Op FileSafe. I determined risks that a sweep of all MPS premises to locate files would result in:

(i) Untrained staff making incorrect assessment of material and incorrect disposal options;
(ii) Failure to record recovered material;
(iii) Failure to record when material was destroyed and why;
(iv) Failure to record what material was submitted to deep storage;
(v) Ongoing failure to comply with MOPI/Data protection/CPIA/Inquiries legislation due to lack of accurate records; and,
(vi) Overloading Records management branch through additional submission of material leading to a failure to check submission to registry and ensure archived material is appropriately recorded on searchable systems.

34. The strategic direction of Op FileSafe was altered to extend the duration of the operation in order to complete preparatory work and enable gradually cascaded and effectively supported delivery. Key strands of Op FileSafe have included:

(i) Review of Records management policy and provision of a more accessible toolkit and guidance for staff;
(ii) Development of a corporate Information Asset Register (IAR) with provision of an interim IAR solution to enable improved asset recording pending delivery of longer term IT solutions;
(iii) Reviewing the use of corporate real estate for document storage and implementing more cost effective solutions to store local archive material;
(iv) Developing systems to ensure material submitted for deep storage is quality assured and recorded on submitting BOCU IAR;
(v) Prioritising buildings scheduled for disposal to ensure held material is disposed of appropriately and corporate real estate programme is not delayed; and,

Signed: [redacted] **Date:** 29th July 2016

(vi) Engagement with units assessed as holding material likely to be relevant to the UCPI.

35. The most significant change to the strategy of Op FileSafe was the decision to support the roll out of the new Records Management policy on an incremental basis with support from a dedicated Records management (RM) branch team. This support includes training and supporting locally assigned staff to review local archives and deep storage collations, sweeping estate for incorrectly filed material and inputting records on interim IAR and RMS systems. The use of a dedicated and trained team was felt necessary to mitigate the risk of material relevant to UCPI, or other inquiries, being missed. The RM team are briefed to identify any such material to AC-PIT. It is of note that Op FileSafe have been contacted for advice and assistance in relation to material located in building sweeps but have to date, received no such reports in relation to UCPI relevant material. I consider that this may reflect the likelihood that such material will have been correctly submitted to GR rather than incorrectly held in local archives.

The five specific issues raised by the UCPI

36. In the following section I will respond to the specific questions raised by the Inquiry:

(1) Details of all requests or instructions by you to your staff to preserve MPS documents for the purposes of this inquiry

37. Instructions that material potentially relevant to the UCPI should be retained and brought to the attention of AC-PIT have been disseminated throughout the MPS by means of presentations and e-mails to senior leaders (Chief Superintendent and above); Intranet communications to all MPS officers and staff; and, specific instructions to Borough Operational Command Units who are responsible for ensuring such messages are disseminated and complied with by appropriate staff

Operation FileSafe briefings

38. Through delivery of Op FileSafe there has been considerable engagement across the MPS to achieve the objectives of this operation, which support the aim to identify and preserve documents relevant to the UCPI. A series of planning, steering and working group meetings were held between July 2014 and April 2015 to progress Op FileSafe. Separate Steering and Working groups were held monthly including representatives from Records Management, Territorial Policing, Specialist Operations, Specialist Crime and Operations, Digital Policing, Shared Support Services, Total Technology programme, Property Services, Directorate of Professional Standards, Met HQ, Training, Directorate of Media and Communications and Met Prosecutions. The subject of providing disclosure to the UCPI was discussed in relation to the business need to deliver Op FileSafe. The Initial Viability Assessment for acquiring an Information Asset Register (D782 section 2.5) makes reference to preparing for the UCPI as a business need. Between June and August 2015 monthly project tracker meetings were held to monitor progress of Op FileSafe delivery.

39. It is important to note that the wider work to improve Information management across the MPS supports the aim of preserving documents without necessarily making specific reference to 'undercover policing.' The instructions and communications that have made specific mention of the need to identify, retain and report material relevant to undercover policing are summarised as follows:

Briefings to senior leaders

40. In 2014 a presentation was developed for delivery to officers and staff of Chief Superintendent rank and above or equivalent staff ranks. This explained some of the issues leading to the UCPI, described challenges experienced in providing disclosure to Mark Ellison QC and outlined objectives and plans for

Op FileSafe. The briefings highlighted that incorrectly filed material with any possible relevance to police corruption, the Stephen Lawrence investigation or undercover policing was to be brought the attention of the Op Beacon team. This presentation was delivered as follows:

- 12.06.14 - Senior police staff from Directorate of Resources, Directorate of Media and Communications, Deputy Commissioner's portfolio (Met Change)
- 07.07.14 - Specialist Crime & Operations (SC&O) Chief Officer Group
- 21.07.14 - Territorial Policing BOCU Commanders and Cluster Commanders
- 01.09.14 - Specialist Operations Chief Officer Group (COG) (D742)
- 22.10.14 - Local Service Delivery Managers (LSDM) responsible for records management delivery at a BOCU level in relation to non-charged case files and other material
- 26.11.14 - Met Prosecutions Senior Leadership team (responsible for management of case files where charges brought and non-charged sexual and serious violence case files)
- Progress reports on delivery of Op FileSafe were regularly provided to AC Hewitt and DAC Taylor via e-mail and discussed at the Op Beacon Gold group.

41. Further senior level briefings delivered in relation to Op FileSafe and making reference to the need to identify and retain material potentially relevant to the UCPI include:

- October 2014 - Briefing to Senior Leadership Team at Croydon regarding Op FileSafe pilot.
- 02.02.14 - Op FileSafe briefing to SC&O8 Op Trident Senior Leadership Team
- 06.03.15 - Op FileSafe briefing to Senior Leadership Teams at Hammersmith & Fulham BOCU

Signed: [redacted] Date: 29th July 2016

- 16.03.15 - Op FileSafe briefing to Senior Leadership Team SC&O1 Homicide BOCU based at Barking
- 17.03.15 - Op FileSafe briefing to Senior Leadership Teams at Barnet BOCU
- 24.03.15 - Op FileSafe briefing to Senior Leadership Team at SO6 Parliamentary and Diplomatic Protection BOCU
- 02.04.15 - Op FileSafe briefing to Senior Leadership Team Met Training and SC&O1 Homicide BOCU based at Hendon
- 13.04.15 - Op FileSafe briefing to Senior Leadership Teams at Newham BOCU including SO18 City airport and SC&O17 Sexual Offences BOCUs
- 16.04.15 - Op FileSafe briefing to Senior Leadership Teams of Central Communications Command based at Hendon
- 28.04.15 - Op FileSafe briefing to Senior Designated Officers for MPS premises in Barnet BOCU
- 13.05.15 - Meeting with Senior Leadership Team at National Domestic Extremism Disorder Intelligence Unit (NDEDIU) regarding UCPI
- 30.04.15 - MPS Information Assurance and Security Board update on Op FileSafe.
- April 2015 – Meeting with Ch Supt heading HQ Strategic Design authority.
- 15.07.15 - MPS Information Assurance and Security Board receive update on Op FileSafe and recommendation to employ Agency staff to support delivery due to lack of capacity in MPS Records Management unit and LSDM teams (D758).
- 07.10.15 – Briefing note provided to AC Hewitt for use in updating Management board in relation to UCPI (D748)

E-mail communications to senior leaders

42. The following senior individuals were emailed with instructions.

- 26.03.2014 - DPS OCU Commander emails all DPS SMT instructing no material is to be destroyed other than very routine documents (D740). This e mail was sent prior to commencement of Op FileSafe.
- During 2014 BOCU Commanders were requested to conduct interim reviews of records management compliance pending roll out of Op FileSafe. Directions included a reminder to bring any incorrectly filed material identified relevant to UC policing to the attention of the AC Public Inquiry Team.
- 29.07.14 - Directions e mailed to TP BOCU Commanders (D741).
- 01.08.14 – Directions e mailed to SO and SC&O BOCU Commanders (D746)
- 11.08.2015 - Email from AC Hewitt to Management Board outlining requirements of the UCPI. States that all material relating to UCPI must be retained and preserved and requesting the message be disseminated (D744).

MPS wide instructions

43. Instructions were disseminated throughout the MPS in the following ways:

- 01.2015 - Intranet article "Following the Paper Trail" drawing attention to refreshed Records Management policy (D780).
- 01.2015 - Intranet 'Policy Notices' features refreshed Records Management policy.
- 01.2015 - 'The Brief' weekly email to senior manages features refreshed Records Management policy. Action for teams to be briefed and policy implemented (D778 & 779).
- 02.2015 - Intranet 'Met Change Weekly' features refreshed Records Management policy. Action for teams to be briefed and policy implemented (D789).

- 02.2015 - 'The Job' features article "Getting Sorted" which describes activity at Op FileSafe pilot site in Croydon. States that the destruction of material should be appropriately recorded (D776).
- 27.03.2015 - Op FileSafe intranet page is launched containing Records Management Toolkit, briefings, policy and instructions for implementation published on dedicated Intranet site. Process diagram requires reviewing staff to consider whether material linked to undercover policing and proforma included to refer such material to Op Beacon/FileSafe team.
- 16.05.2014 - Intranet article "How to manage your documents and records" circulates summary of good practice, refers to MOPI, states need to record disposal decisions including rationale and for information to be stored in a searchable and retrievable location (use of S rather than H drive) (D777).
- 05.2015 – Policy Notice 05-2015 Informs staff of replacement of Records Management Manual v8 with Records Management Toolkit (D783).
- 07.08.15 – Intranet article "Exiting EDH – Let's start preparing" Placed on DoI pages to provide guidance to staff on how to prepare for moving premises. Refers to RM and Op FileSafe briefing note and emphasis need for proper review prior to destruction (D750)
- 11.08.2015 - Intranet article "Be Ready to Respond to the Inquiry into Undercover Policing". Front page article viewed by all staff on logging on to Aware. Article refers to terms of reference and requirements of the Inquiries Act, including the obligation to keep any documentary or otherwise stored relevant material (D747)
- 2015 - 2016 – Records Management deliver series of Op FileSafe briefings to 108 departmental Single Points of Contact during implementation. Requirement to refer material relevant to UCPI highlighted (D752)
- 2015 - 2016 - Records Management deliver series of Op FileSafe briefings to 250 officers from SC&O and Met Prosecutions as part of a

Signed: [redacted] **Date:** 29th July 2016

training package for Records Management System (RMS). Requirement to refer material relevant to UCPI highlighted (D775)

BOCU instructions to specific units

44. Instructions were disseminated to or by Borough Operational Command Units (BOCUs):

- May 2014 – SO15 circulate policy instruction in relation to upcoming Inquiry into undercover policing that 'No member of this Command or Digital Policing, should delete from any SO15 information system any registered files, records or electronic information of possible relevance to these matters (paper, electronic or other) without the authority of Commander SO15' and that;
    - No member of this Command or Digital Policing, should delete from any corporate system any SO15/ SO13/ SO12 related material of possible relevance to these matters from any other information system, any registered files, records or information (paper, electronic or other) without the authority of Commander SO15 (D751).
- Oct 2014 – AC-PIT engage with SO15 re Retention, Review, Disposal of SO15 records (D749).
- Apr 2015 – Op FileSafe team engage with SO15 re scoping of existing Information management systems and business case for dedicated Review, Retention and disposal team. Engagement includes discussion of Op FileSafe objectives and requirement to provide disclosure to UCPI.
- May 2015 – SC&O35 circulate BOCU wide instruction that no material relevant to undercover deployment is to be destroyed without written authorisation of the BOCU Commander SCO35.
- June 2015 – The Head of Compliance and Assurance at National Counter Terrorism Policing HQ (NCTPHQ) submitted a briefing document to AC Hewitt (MB lead for Information Assurance and

Signed: [redacted] Date: 29th July 2016

Security) that set out a number of information risks held by SO15 and proposed steps to improve Information management. The proposals include a number of areas for where records should be submitted to more robust Retention Review Disposal (RRD) procedures. NCTP HQ highlight that external interests in older SO15 records, including the UCPI, mean that there are conflicting expectations regarding whether material can be deleted. For example disposal of IMOS records has been halted due to the requirements of Op Herne/UCPI. SO15 propose that none of the potentially relevant files, particularly those held in IMOS and older BRS records, be signed off for destruction at present (D754). This approach was agreed by AC Hewitt. It is of note that the requirements of the UCPI and other legacy investigations have directly impacted plans to review and dispose of material in compliance with other legislation and business need.

- 2 June 15 - SC&O35 issue instruction to staff to retain all material of potential relevance to UCPI (D743)
- July to Oct 2015 – SO15 liaise with Op Beacon/FileSafe re planned displacement of IMOS from NSY for building disposal. Decision made that material will not be submitted to deep storage and will be transferred to [redacted] for duration of UCPI to ensure accessibility and limit risk of material being misplaced (D753).
- 09.11.2015 - SO15 instructed by AC-PIT to preserve all SO15 duty states for duration of UCPI (D745)

(2) Any steps that have been taken to verify that any request or instruction to preserve documents is being complied with

45. In considering what steps have been taken to ensure compliance I refer the UCPI to my response to Question 1 which describes the measures taken to raise awareness of the UCPI and obligations under the Inquiries Act 2005 across the MPS. My description of activity undertaken through Op FileSafe is also directly relevant to this question as it describes activity to improve understanding of Information management systems and processes and to

Signed: [redacted] **Date:** 29th July 2016

improve the recording of material held to ensure it can be located when requested. Op FileSafe has resulted in units contacting AC-PIT in relation to material found for advice regarding its appropriate disposal, to date none of these reports have related to material relevant to the UCPI.

46. Further activity conducted by AC-PIT includes the following:

(i) AC-PIT has been established as the single point of contact (SPOC) between the MPS and Directorate of Legal Services legal team. All Rule 9 directives received from the UCPI are reviewed by DLS and a schedule provided to AC-PIT of what enquiries are required to complete a response. AC-PIT use the HOLMES Major Inquiry system to record activity in response to Rule 9s. An action is raised and where searches for relevant material are required consideration is given to setting search parameters and/or schedules. For some requests, such as material from Op Herne's systems, AC-PIT have full and unrestricted access to the relevant systems and will complete searches and recover material themselves. For other requests, such as current policies requested in Rule 9(4), relevant material is held on databases to which AC-PIT staff do not have either the access or the knowledge of the material to ensure comprehensive disclosure. In these instances AC-PIT make an initial determination of what units may hold relevant material and make contact with appropriate staff from those units. Meetings are held to discuss the requirement, highlight the legal obligations to comply and explain to units how sensitive material will be handled and disclosed. The UCPI should be aware that the extent of disclosure of sensitive material required by AC-PIT is unprecedented and liaison is required to ensure staff comply with disclosure demands which run contrary to their training and previous experience. In relation to Rule 9(4) AC-PIT assigned officers to work alongside SC&O35 and SO15 staff to review their systems and identify relevant material. Both units allowed access to AC-PIT for this exceptional purpose. My experience of providing disclosure has been that the most effective

Signed: [redacted] Date: 29th July 2016

way to ensure all relevant material held by specialist units is to provide clear written direction to the holding unit and support them in conducting the relevant research and provide disclosure. Attempts by AC-PIT officers to research unfamiliar systems in relation to subjects they have limited knowledge of are likely to result in material being missed.

(ii) Acquisition of Relativity based eDiscovery and document management platform. The UCPI has been extensively briefed on the Relativity based system which I have identified and acquired to use as the primary document management system for providing disclosure to the UCPI. While the effectiveness of this system is clearly dependent on the ability of AC-PIT to identify, locate and copy relevant material onto the system it is relevant that a considerable financial outlay is being made by the MPS to provide the Relativity platform and the CT Holmes case management system. These systems are assessed as providing the best available facilities to record activity in response to the UCPI requirements for disclosure and to maintain a fully auditable record of all review, search and redaction activity undertaken in relation to material copied onto the Relativity system. The use of external vetted IT contractors to assist in operating Relativity will provide the ability to provide independent evidence of how the system has been used to copy, search and process material.

(iii) Completion of Atlas of relevant IT systems and databases – AC-PIT have researched current IT and archive Information systems in use by the MPS to determine which may potentially contain material relevant to the UCPI. The Atlas includes name of current systems relevant to the UCPI with details of SPOCs, data type, primary nature of content, a brief description of the system, estimated size of data held, accessibility, limitations of search function, dates of operation, whether material has been migrated from/to other systems and whether it is a corporate or vulnerable non-corporate system.

Signed: [redacted] Date: 29th July 2016

(3) The steps that have been taken to address the risk that individual officers or staff may deliberately seek to destroy or amend parts of the record, and to ensure that any such attempt will be prevented or detected

47. MPS AC-PIT has been established to provide a dedicated team of officers to ensure full and comprehensive disclosure to the UCPI. Officers selected to the unit are subject to SC level vetting and [redacted] no officers on the unit have served as a UC.

48. In considering what measures could be taken to prevent deliberate destruction of relevant material in relation to non-SDS/NPOIU undercover operations it is important to consider the potential scope of relevant material in relation to a terms of reference as broad as 'all undercover police operations since 1968.' The two most clearly identifiable groups of material relate to digital and paper exhibits relevant to the operations of the SDS and NPOIU. A scoping exercise conducted by AC-PIT in 2015 identified 89 databases and paper based archives in current use by the MPS that could potentially contain material relevant to the wider subject of all undercover policing operations. This does not include now obsolete IT systems the content of which may not have been migrated to current systems. The various identified databases and archives vary in purpose, accessibility and ability to monitor activity in relation to them. I will summarise the position in relation to key sources of material:

    (i) Material related to SDS operations - In relation to material relevant to the SDS Op Herne have been engaged in identifying and recovering material since 2011. Material recovered is secured in Op Herne's exhibit storage system. Digital material is held in original exhibits and the content copied onto Op Herne's case management and forensic IT systems. The UCPI has previously been briefed in relation to these systems so I do not propose to describe them further as that is more appropriately a task for Op Herne. However, in terms of preventing

Signed: [redacted] Date: 29th July 2016

destruction of this material it is my belief that Op Herne's IT and exhibit storage systems are secure and accessible only to officers assigned to Op Herne and AC-PIT. Seperate CT Holmes case management accounts are in use by Op Herne and AC-PIT. The Op Herne account can be accessed by officers and staff assigned to Op Herne and AC-PIT. The 'Pitchford' account used by AC-PIT can only be accessed by AC-PIT officers and staff who have received Holmes training and been granted user access by the AC-PIT Office Manager. Officers trained to 'View only' standard can log on, search and view documents (of all types) up to the security level they have been granted. In most instances the default is level 4. The do not have the ability to register new material, move or delete material already registered to the Holmes Incident. Officers and staff with CID user and Indexer access can delete documents but cannot delete Actions or Exhibits which cannot be deleted once entered on Holmes. If required audits of activity can be conducted by document number, terminal asset number or user ID which would establish who deleted what, when and from which terminal and could be used to determine if material had been inappropriately deleted.

(ii) Material related to NPOIU operations - In February 2013 Op Herne obtained the NPOIU material relating to [redacted] **[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 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

Signed: [redacted] **Date:** 29th July 2016

exhibits relevant to the NPOIU are held in Op Herne's secure exhibit system.

(iii) General registry (GR) – Documentary archive where the large majority of case files of investigations involving the undercover tactic are held. Files are recorded on the Record Management System (RMS). This system is widely accessible to enable local staff with Information management roles to input records on the system. RMS cannot be searched for case files relevant to operations where undercover tactics were used as this is not a search category used on RMS, nor would it be appropriate to mark files as relevant to use of a covert technique for reasons of operational security. Registry files are reviewed for destruction by GR staff once they reach their MoPI destruction date. A decision to destroy is not automatic once the date is reached. GR staff will conduct review of the material first to determine if appropriate to destroy. The extent of review will vary with the nature of the material with the highest level review being conducted on case files in relation to serious violence and sexual offences. GR files can be requested by officers but a record is kept in RMS of who requested the file and when it was provided.

(iv) Local archives – As previously described a significant organisational risk has been identified in relation to inadequate recording of material held in local archives and an inconsistent approach to what data is recorded and material held. Op FileSafe is underway to locate incorrectly filed or retained material and ensure it is appropriately filed or destroyed (D755). The work underway to improve Information management of paper and portable data storage archives has been described previously in this statement under Op FileSafe. During the course of Op FileSafe a review of security arrangements at the new MPS deep storage facility has been completed by Records Management branch (D756 & 757).

Signed: [redacted] Date: 29th July 2016

(v) INFOS – This IT system is used for a range of purposes in relation to covert policing including records of undercover deployments. It contains records of Advanced level operations since 1999, Foundation level operations since 2007 and Covert Internet Investigator operations since 2008. This system is only accessible to a small number of vetted personnel. System entries are not subject to routine deletion. The only way an entry can be deleted is through liaison with the Secure systems team in Digital policing who can conduct the deletion. Only one member of staff in SC&O35 has authority to direct such a deletion. Staff have been briefed in relation to the UCPI. A directive has been issued to SC&O35 staff to retain all potentially relevant material for the UCPI due to the possible significance of this units records (D743).

(vi) Information Management Operational Support (IMOS) – Paper archive of Special Branch files catalogued and indexed on an IT system. Access to this system is restricted to a small number of vetted personnel within SO15. The IT index system retains records of documents held and can be used to identify any physical document that has been removed from a file. SO15 have been engaged with by AC-PIT re retention of IMOS material and a policy decision made to suspend all destruction of material held for the duration of the UCPI. A further policy decision has been made to retain the IMOS archive in a secure location in inner London for the UCPI to maintain accessibility. These decisions have generated a significant cost to the MPS. It is likely that, were it not for the Pitchford and Goddard Inquiries a large proportion of this material would be subject to either destruction or submission to deep storage.

(vii) Informant Management System (IMS) – SC&O35 CHIS files are held on an IT system which has been in use for around 15 years. Files prior to that are held on paper, Op FileSafe are currently assisting SC&O35 to record these files on an IAR and transfer them to secure [redacted] **[gist: storage]**. A total of 280 staff have access to the

Signed: [redacted] **Date:** 29th July 2016

SC&O35 IMS system but only 15 staff have access to the entire system and can search outside their own unit files. The server is securely held and requires [redacted]. It is not possible for any member of staff to delete an IMS file once it has been authorised and all views of material are recorded on the system. The SO15 IMS system is held on paper files stored in a [redacted] **[gist: secure]** environment only accessible to [redacted] **[gist: vetted]** staff who are controllers and handlers on the unit.

(4) Details of any instance in which you suspect that any officer has circumvented, or sought to circumvent, the steps taken

49. I am aware of an allegation in relation to deletion of records relating to Baroness Jones (which is the subject of a separate rule 9 request by the UCPI). If substantiated this may lead to criminal or misconduct proceedings. The material in relation to this allegation and the MPS response to it is to be provided in the response to the rule 9 request that specifically relates to it. Other than this issue I am not aware of any instance where an officer has been suspected of circumventing or attempting to circumvent the steps taken described above.

(5) The ways in which routine or automated document destruction procedures have been modified to ensure that relevant documents will not be destroyed

50. The MPS does not use automated document destruction procedures in relation to documentary archives, see para 14. AC-PIT have identified 89 documentary and IT information management systems in use by the MPS as holding material of potential relevance to the UCPI. The only one of these systems with automated deletion of records is National Strategy for Police Information Systems (NSPIS). This is the national system for criminal justice case management and is not controlled by the MPS.

Signed: [redacted] **Date:** 29th July 2016

51. Since July 2015, 458 officers and staff have been trained on the requirements of Op FileSafe. Training for officers and staff engaged in the review of material held in local archives and recalled from deep storage for review has included the need to identify and retain material linked to undercover operations. This is not a straightforward task as case files are primarily catalogued by offence type, not in relation to what tactics were used in the investigation. The Op FileSafe process map used by staff for review of material makes specific reference to the need to consider whether the material relates to the subject of 'undercover policing' and to retain and report such material to AC-PIT using the provided pro forma. Other types of material have been flagged up to AC-PIT but no incorrectly filed 'undercover policing' material has been reported. This may reflect the tighter controls implemented on storage and archiving of sensitive material relevant to covert policing tactics. However it may also be due to the inherent difficulty in identifying material relevant to a covert tactic.

52. In relation to material relevant to the ToR of the UCPI, General Registry have been fully briefed on the requirements. The head of General Registry was fully engaged with Op FileSafe, up to his retirement in December 2015, and ensured the Operational requirements of FileSafe were built into local processes. The current premises used to store the bulk of GR material are scheduled for disposal under the MPS Corporate real estate programme. Since January 2016, MetHQ Records Management have had a team embedded in GR to work through and log all records contained in the secure areas prior to removal to the new storage facilities. This team is fully aware of the requirements of Op FileSafe, the need to properly record all files and to flag to AC-PIT any files of specific interest to the UCPI. The large majority of cases involving undercover tactics will involve crime types (cuts) attracting MPS MoPI retention periods of 12 years and potentially 30 to 100 years.

53. Op FileSafe intervention has found that application of formal review of local archives is currently sporadic and generally only takes place when a record is due for disposal. Exceptions to this include all serious, sexual and violent

Signed: [redacted] Date: 29th July 2016

crime groups of material (cuts) which are currently reviewed by Met HQ Records Management as part of the legislative requirement under the Public Records Act. The RM team is currently reviewing all such files from the late 1980s working up towards the current date and recording decisions on continued retention, transfer for permanent preservation at the National Archives or disposal. MOPI group 3 records are currently liable to time based disposal. The entire review process is being overhauled to align with the requirements of the College of Policing (CoP) Information Management Authorised Professional Practice (APP). The MPS is currently working with the (CoP) in order to refresh the MPS Records Management policy / toolkit between February 2016 and April 2016. This will bring MPS retention periods in line with the CoP APP. With regard to MoPI Group 1 and 2, the MPS intends to undertake scheduled 10-year reviews, also supplemented by triggered reviews (i.e. by an Freedom of Information Act or Subject Access Request) following the NRAC (National Retention Assessment Criteria) template (D785). With regard to MoPI Group 3, the MPS intends to adopt time-based disposal for minor offences (e.g. shoplifting), but certain crimes (those involves any element of violence or other harm-based concern, i.e. common assault allegations) will be subject to review. This policy review in 2016, once confirmed and adopted, will bring the MPS in line with MPS APP.

54. As part of Op FileSafe, all material currently held by the MPS is being reviewed prior to disposal. Practice prior to Op FileSafe was to review MoPI Groups 1 & 2 at the end of their retention period and for time based disposal of MoPI group 3 (volume crime) after 12 years. All legacy records are being reviewed between now and March '17. This intervention by Op FileSafe will be augmented by a policy update that enshrines an ongoing and consistent review process.

55. Met HQ Records Management are programming MPS Information Assurance audits for each area to be conducted from six months after completion of the Op FileSafe training and intervention at each BOCU. This internal audit programme will report back on progress at regular quarterly meetings with

RM. Initial audits have already been undertaken around selected areas such as the management of registered files. These results have been made available to Op FileSafe and RM to enable the development of policy update and improved training.

56. I have considered the possibility of cross referencing INFOS records of UC deployments to RMS records to identify where the deployments have led to case files being generated and arranging for those files to be placed in a separate and secure collation within GR. I have not undertaken this work due to:

(i) Lack of available resources to review all INFOS records and identify related case files. There are a large number of potentially relevant INFOS records and further research would be required to identify operations pre-1999. Such an exercise would be highly resource intensive;

(ii) The UCPI are unlikely to wish to review the vast majority of the files that would be identified;

(iii) Locating the files in registry and transferring them to a separate location would have a cost implication and would be a major demand on the time of GR staff who are required to review, quality assure and archive material located and submitted through Op FileSafe. Separate storage of potentially 2000 plus case files relevant to complex investigations would require a large secure storage facility;

(iv) The files are securely held in GR and can be located and recovered if required by the UCPI. Any files currently misplaced from GR are likely to be located by Op FileSafe which has recovered 500 GR files to date.

(v) Case files vary greatly in size depending on the length and complexity of the investigation. The majority of material held in each file will not relate to the use of the undercover tactic. As an example the case files relevant to the Rachel Nickell murder investigation are held in over 90 crates the majority of which are unlikely to be of relevance to the UCPI. The case file will have a retention period of 100 years minimum.

Signed: [redacted] **Date:** 29th July 2016

I now wish to add as follows to my previous statement of 26th January 2016-05-13

57. Update to paragraph 11 of my previous statement. The MPS Digital Policing department is currently engaged in a major project to transform the delivery of information technology services to the MPS. This Digital Policing Target Operating Model (TOM) aims to improve the efficiency and effectiveness of MPS IT and provide fit for purpose services for front line policing and police support. The aim is to implement the TOM by the end of March 2017.

58. Update to paragraph 13 of my previous statement. In this paragraph and others in the statement I refer to 'vulnerable non-corporate IT systems.' I wish to clarify that the term vulnerable is used to refer to risks that exist around ongoing maintenance support and integration of these systems and is not a reference to security risks.

59. Clarification to paragraph 18(iii) of my previous statement. 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 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

Signed: [redacted] Date: 29th July 2016

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.

60. Correction to paragraph 25 of my previous statement. In this paragraph I state that there has never been any dedicated resource for delivery of Op Filesafe. The correction is that following an application for resources to MPS Management Board an allocation was made to recruit a team of 9 Agency staff to work with Records Management branch and locally deployed officers and staff on delivery of Op Filesafe. The first of these staff commenced work in December 2015 and all nine were in place by January 2016. The Records Management team are supported in reviewing material held in archives and deep storage by officers and staff deployed by the BOCUs whose material is under review.

61. Update to paragraph 35. This paragraph states that to date Op Filesafe has received no such reports of UCPI relevant material located in building sweeps. To update the Op Filesafe team have located such material while assisting BOCUs to review local archives and have ensured the material is retained. Since completing my earlier statement AC-PIT have been informed of a considerable quantity of potentially relevant material held in one local archive and are currently working with Op Filesafe to preserve and catalogue this material.

62. Update to paragraph 43. This paragraph lists MPS wide instructions to staff. In May 2016 BOCUs were instructed that over seven days they are to include on the formal briefings disseminated to all officers a reminder to staff of the requirement to ensure that no material is destroyed or deleted under any circumstances if potentially relevant to undercover policing. A direction was posted to all staff on the MPS Intranet system on 20 May 2016 in relation to Records management policy which included an instruction that no material

Signed: [redacted] **Date:** 29th July 2016

relevant to undercover policing is to be destroyed or deleted under any circumstances.

63. 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 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.

64. Correction to paragraph 48(v). In this paragraph I state that SC&O35 staff are unable to delete material from INFOS. At the time of completing my earlier statement this was the understanding of SC&O35 staff and myself. Digital Policing have since clarified that a small number of staff with higher level access can delete material from INFOS and have explained to SC&O35 Support Manager the process to do so. As far as the SC&O36 Support Manager is aware no such deletion of records of undercover operations has ever been done.

65. Update to paragraph 48(vii). In this paragraph I highlight the SO15 maintain a separate system for recording information related to CHIS handling, management and intelligence. I wish to update that the MPS Directorate of Professional Standards (DPS) also maintain a separate system for the same purposes.

66. Update to paragraph 49 of my previous statement. In this paragraph I state that I am aware of one instance whereby any officer may have circumvented, or sought to circumvent, steps taken to preserve material. Since completing this statement I have become aware of a further separate incident and have ensured that the UCPI have been made aware. This incident is currently subject to investigation. The UCPI will be kept informed of progress. Both incidents that I am aware of took place prior to the commencement of the UCPI in July 2015 but after the circulation of instructions to officers and staff to preserve material of potential relevance to undercover policing. I also wish

Signed: [redacted] Date: 29th July 2016

to clarify that while the investigation did treat the allegation as a potential criminal or misconduct matter at the point when I completed my previous statement the investigation had concluded with no offences or conduct matters being identified.

67. Update to paragraph 51. Since completing my previous statement UCPI relevant material has been located incorrectly archived as described in paragraph 61.

68. Correction to paragraph 53 of my previous statement. The last line of this paragraph states that 'will bring the MPS in line with MPS APP.' This is an error and should read 'will bring the MPS in line with College of Policing APP.'

69. Update to paragraph 54 of my previous statement. This paragraph states that all legacy records are being reviewed under Op Filesafe. To date around 500,000 files held in local archive and deep storage have been reviewed and RMS used to create a standardised and searchable record of files. It is estimated that the operation will conclude in 2017 by which time the MPS will have a greatly improved compliance with data protection legislation and MoPI. Op Filesafe will generate a more effective and searchable record than currently exists of material held in deep storage and local archives and is anticipated will locate the large majority of files which have been lost, misplaced or incorrectly archived.

70. Correction to D743 appendix to my previous statement. This appendix includes an e mail sent to staff on SC&O35 which states that the retention period for material is 100 years. This is incorrect. Some police material can attract retention periods of 100 years including that directly relevant to Public Inquiries. The author of this e mail mistakenly believed that this retention period therefore applied to all material held by their unit.

71. Update to D754 appendix to my previous statement. This report in relation to Management of Information within SO15 identifies a number of risks in

Signed: [redacted] **Date:** 29th July 2016

relation to Information systems. The risks identified in the report in relation to IT systems are currently being addressed through a major national project to address vulnerabilities in IT systems used by counter terrorism units. The section of this report relating to hard copy material stored at TNT states 'Records Department have not yet been able to establish how much material each OCU, including SO15, have stored.' Under Op Filesafe all OCUs will review their collations at TNT to address this issue.

72. Correction to Appendix 1 of statement. The first entry on the appendix stating DSU Hutchison appointed to lead is duplicated in error as the third entry.

I now wish to add as follows to my previous statement of 3rd June 2016

Updates and clarifications

73. Correction to first line of my statement of 3rd June 2016. The first line states that I submitted my first witness statement in response to rule 9(8) on 26th January 2016. I wish to correct this date to 29th January 2016.

74. Update to paragraph 18(v). This paragraph states that the minimum retention period for case files relevant to undercover operations is 12 years. The MPS are currently in the process of reducing this retention period to 7 years with disposal at the end of this period for high volume non-violent offences (MoPI group 3), for example low value theft. This change will bring the MPS into compliance with national MoPI standards. Case files relating to serious crime (MoPI groups 1 and 2) will continue to attract longer retention periods of 12 years and above depending on the crime type under investigation. Such files are scheduled for review every 10 years throughout their specified retention period which can be anything up to 100 years. There is an additional facility to allow triggered reviews at any point throughout their retention.

75. Correction to paragraph 20 and paragraph 50. These paragraphs both state that the MPS does not operate any automatic destruction processes. This was

Signed: [redacted] Date: 29th July 2016

the case until 2016 and remains the case for MoPI group 1 and 2 files which remain subject to review before destruction. The process in relation to MoPI group 3 described in paragraphs 53 and 54 involves automatic destruction of such files at the end of their retention period. This was previously 12 years but is being reduced to 7 years at present. It is possible that files relevant to some undercover deployments could exist in MoPI group 3 and therefore be at risk of automatic destruction. For example, deployment of a foundation level undercover officer to pose as purchaser of stolen property of low value. I have discussed this risk with the head of MPS Records Management. AC-PIT are currently reviewing information held in relation to undercover operations. Information recovered will be cross-referred by AC-PIT against RMS and, if necessary, local archives, to locate and secure the relevant files.

76. Update to paragraph 20. In this paragraph I describe paper files held in local archives or 'file on division.' I wish to point out that case files relevant to crime investigations should only be held in local archives or 'file on division' if MoPI group 3. Administrative material under MoPI group 4 (miscellaneous) is also usually appropriate to be held in local archives. Case files relevant to investigations of more serious crimes under MoPI groups 1 and 2 should be submitted to GR. However, work conducted for Operation Filesafe has identified that this policy has not been fully complied with over many years resulting in significant quantities of MoPI group 1 and 2 files being located in local archives. Due to the work of Operation Filesafe these files are now being recorded under RMS and transferred to GR.

77. Correction and update to paragraph 50. In this paragraph I state that the only IT system in use by the MPS with automated deletion of records is NSPIS. Since completing my earlier statement I have sought further information around this system and am advised by Met Detention that custody records held on NSPIS are archived by the commercial operator of the system. I have not yet been able to confirm with the commercial provider what the process is for archiving records and how the MPS could recover any such records. As the system was only introduced in 2005 it is unlikely that any custody records

Signed: [redacted] Date: 29th July 2016

held on it would have been considered for RRD as until the recent change to MPS retention periods described in paragraph 71 records related to crime investigation attracted a retention period of at least 12 years. I have directed a spot check of records from 2005 at the BOCU that first introduced NPSIS in the MPS. Custody records related to even very minor offences are still present on the system and therefore recoverable.

78. Update to paragraph 55. I am informed by the MPS Head of Records Management that he intends to augment the internal audit programme referred to in this paragraph with a MoPI self assessment process for BOCUs to complete. He has also commenced contact with the National Archives Information Management Assessment team to establish an external audit process.

79. Correction to paragraph 60. I am informed by the MPS Head of Records Management that he did not find it necessary to recruit outside Agency staff for the Operation Filesafe team as he was able to arrange for re-deployment of nine MPS police staff to form this team.

80. Update to paragraphs 69. I am informed by the MPS Head of Records Management that the anticipated date for conclusion of Operation Filesafe review of local archives and deep storage is now March 2018.

Verification following rule 9(12) request

81. The following steps have been taken to verify that the instructions given to officers to preserve material relevant to the UCPI has been received and followed:

   a. In relation to AC-PIT officers and staff, I and the AC-PIT Detective Inspectors have ensured that the importance of the message relating to document preservation by verbally reinforcing the message at AC-PIT regular meetings. This reinforcement and the measures relating to

Signed: [redacted] Date: 29th July 2016

document handling set out at paragraph 32 of my statement in response to rule 9(10)(a) mean that I believe the message has been received and is acted upon by AC-PIT officers and staff.

b. In relation to GR, I am informed by the head of Records Management that he has verbally reinforced the importance of preserving documents to each member of the GR staff involved in RRD decision-making, reinforcing the message to preserve relevant documents.

c. In relation to IMOS, I stated the following at paragraph 49 of my statement in response to rule 9(10)(a):

"*There is a direction in place that no material held by IMOS will be subject to destruction or deletion while the UCPI is ongoing. This is a suspension of the RRD process. This has been justified as an exception to the Management of Police Information requirement not to hold information once it does not serve a policing purpose on the basis of the potential relevance to the UCPI.*"

This is relevant to the present request as any destruction of documents would be noticeable. I am not aware of any such destruction having taken place. I therefore think that the message of retaining documents has been received and followed at IMOS and there is a measure in place that helps to prevent inadvertent destruction of relevant material.

d. I am informed by the head of Records Management that the staff and officers working on Operation Filesafe have been briefed verbally at meetings to ensure that the requirement to preserve documents relating to the UCPI is understood and followed. These individuals oversee large scale office moves and will intervene if relevant documents would otherwise be destroyed. I am aware of two occasions when people working on Operation Filesafe have prevented material from being destroyed though this was not material relevant to the

Signed: [redacted] Date: 29th July 2016

UCPI. I have personally been contacted by units conducting reviews to ask for advice on the process to follow and potential relevance of material which indicates to me that the message to preserve relevant documents has been received and understood by those individuals.

e. In relation to the wider MPS workforce, I directed Operation Filesafe be conducted on a staggered basis to ensure that BOCUs received appropriate support to implement the new process. The support for Operation Filesafe is intended to ensure that the reviews are conducted in accordance with the Records Management policies and toolkit. To date Operation Filesafe has worked with BOCUs to review over 500,000 files. This volume of work can only be implemented with the support and cooperation of senior leaders who have been briefed and instructed as I describe in paragraphs 40, 41 and 42. BOCU Commanders have allocated staff locally to conduct these reviews assisted by Operation Filesafe. The fact that such a large quantity of material has been reviewed to date indicates to me that the directions described in my statement above have been received and are being acted upon.

82. In addition, the MPS intends to take the following steps:

a. Create a list of known undercover operations which could be used to restrict access to relevant files at GR. This will help to prevent inadvertent destruction of documents by ensuring that those files are not removed from their current location. Access to the list will be restricted.

b. The head of Records Management has agreed periodically to review a sample of the files at GR for which access is restricted for the reason of relevance to the UCPI to see if files are being requested. This should assist in preventing inadvertent destruction.

Signed: [redacted] **Date:** 29th July 2016

c. The head of Records Management has agreed to instruct GR staff to review case files in more detail for relevance to the UCPI when the case file is subject to a RRD decision.

d. AC-PIT are engaged in identifying local archives with relevant material. In this process, the importance of preserving relevant material is reiterated to borough officers and staff that have been contacted, which I believe will help to verify that the message has been understood and followed.

e. The Department of Professional Standards (DPS) has a project in place (running from 2014) to create a fully searchable record of all DPS anti-corruption investigations. This will assist in identifying DPS relevant material, though it is not yet complete. The scale of the operation (to the best of my knowledge, digitising approximately 3,000 crates of documents and costing approximately £1.35 million) means that I do not believe the process can be speeded up for the UCPI nor can further resources be allocated to it for the purpose of the UCPI.

f. To review the measures to ensure that the instructions not to delete material have been received and are followed every six months.

83. I have considered the following further steps:

a. Requesting individual verbal briefing about the UCPI to each MPS officer and member of staff;

b. Preventing all destruction of documents by MPS staff or officers;

c. Checking all documents that are to be destroyed for relevance to the UCPI;

Signed: [redacted] **Date:** 29th July 2016

d. Circulating a list of all known undercover operations widely;

e. Isolating all case files that contain documents relating to the use of undercover policing.

84. I have not decided to take these steps for the following reasons:

a. The measures taken to date are the most effective available ways to spread the message to preserve relevant documents to the largest possible number of staff and officers. My experience is that the intranet is amongst the first port of call for the majority of officers when they start duty and staff when they arrive at work. The home page of the intranet is the home page for web browsers on MPS computer system terminals. Having a message displayed on the home page of the intranet enables the largest possible number of officers and staff to read and consider it.

b. The MPS has a workforce of approximately 42,000 individuals, making personal briefings impracticable. I have however circulated the message to preserve relevant documents on the MPS briefing system (Met Bats) used by all operational units to deliver daily briefings to officers. Met Bats briefings are delivered by supervisors to teams as they go on duty and are regularly reviewed by officers working independently. A combination of Intranet and Met Bats circulations are therefore the most effective means of cascading messages across the force. Individual BOCUs may have circulated their own internal messages to officers and staff such as the direction given to all SO15 officers and staff (D751).

c. Operation Filesafe is a major operation that engages with BOCUs to advise and assist their review of local archives. From members of this operation, the message to present relevant documents is spread to MPS boroughs.

Signed: [redacted] Date: 29th July 2016

d. The day-to-day work of the MPS requires material to be destroyed for good reasons, including preventing sensitive material from being distributed inappropriately, complying with legal obligations such as data protection law and preventing working areas from becoming overloaded by paper. Given the number of buildings in the MPS estate and the amount of paperwork generated by police work, preventing all destruction of documents would affect the ability to run a police station massively.

e. Circulating a list of all known undercover operations is likely to create serious security risks as for some cases the use of the tactic will be operationally sensitive.

f. It is not obvious on the face of many (if not all) case files that undercover policing was used. There is no easy way of identifying case files with relevant information inside. To isolate all such files would require reading all case files at GR and in local archives relevant to crime investigations where the tactic may have been used. This would require a huge team of officers employed full time, which is not something for which the MPS has resources. MPS Records Management report that there are around 1.35 million GR files, each file can vary in size from one sheet of paper to 100 plus boxes of material. The MPS does not have an accurate figure for how many crime investigation files are held in local archives but calculating from total recorded crime against average retention periods generates a figure of around 6.5 million. These figures are only for crime investigation files and do not include files that may contain other relevant information such as policy files, administrative files and personnel files. These figures also do not include general administrative material held in offices which are not required to be categorised or retained under MoPI.

Signed: [redacted] **Date:** 29th July 2016

85. For these reasons my focus has been to improve the searchability and security of local archives, deep storage and relevant systems and to generate records of potentially relevant investigations.

86. The fact that I have not decided to take the steps described in paragraph 83. does not mean that I consider the matter closed. In addition to considering the issue of verifying that the message to preserve relevant material has been received and is acted upon specifically at the periodic review, I remain open to considering other methods and will institute further means to achieve this as appropriate.

87. The UCPI have requested supplementary information which I address as follows:

a. The UCPI have requested further information regarding the Independent Scrutiny panel used by the MPS. This group was established in 2014 to provide independent advice to Assistant Commissioner Professionalism. The group was initially referred to as the Independent Oversight Group. The panel is chaired by Lord Justice Peter Jacobs, the other two members are Margaret Casely-Hayford who works in the voluntary sector and Karen McFarlane who is an expert in public sector information management. The committee will remain entirely independent of the MPS and will not replace or replicate any of the statutory oversight and governance functions of The Mayor's Office for Policing and Crime (MOPAC). The role of the panel is:

   - To provide an independent review and comment on the strategic approach taken by the Public Inquiry Team in response to all of the investigations and enquiries outlined in the introduction above.
   - To provide an independent review and comment on the strategic approach taken by the Public Inquiry Team in

response to any additional taskings or activities as requested by Assistant Commissioner, Professionalism.

- To provide an independent review and comment on developing plans to improve records management and document retention within the MPS.
- Where the MPS are required by any of the investigations or enquiries to provide a specific response, to provide an independent review and comment on the proportionality, thoroughness and openness of the response.
- To provide an independent review and comment on the effectiveness with which emerging organisational learning from the Public Inquiry Team is embedded within MPS practice.
- The committee will receive access to any requested documentation unless a specific and recorded decision by AC Professionalism prohibits such access.
- In order to fully discharge its function, the committee will be able to speak to any MPS employee.
- To provide an independent review and comment on proposed media plans at key points in the work of the Public Inquiry Team.

Whilst the panel exchange with the MPS their comments and views on the approach to the UCPI they have not presented findings, reports or conclusions subsequent to these discussions. It is not anticipated that any such reports will be provided.

b. Update to paragraph 32. This paragraph states that managers responsible for key systems such as INFOS and IMOS have been briefed. There are a large number of systems in the MPS which may contain relevant material as explained previously to the UCPI. Paragraphs 40, 41 and 42 outline briefings delivered to a wide range of senior MPS officers and police staff. These briefings and e mail circulations have highlighted the need to retain relevant material and have effectively covered senior and mid-level managers responsible for systems where relevant material may be held.

c. Update to paragraph 48 (v). INFOS holds detailed records of operations from the years reported in this paragraph. The INFOS systems also holds records relating to undercover operations prior to those dates however these records are incomplete. The earliest of these records identified to date is 1991.

d. Update to paragraph 48 (vii). IMS stands for Informant Management System. The MPS computer database used by SC&O35 for CHIS handling is referred to as IMS. However SO15 and DPS both operate their own separate systems for handling CHIS as I described in paragraph 65. These are also referred to as IMS.

e. Update to paragraph 53. A small number of Records Management staff are engaged in rolling Review, Retention, Disposal (RRD) decisions regarding General Registry files. As I explain in paragraph 81(b) they have been verbally briefed to identify and retain material of potential relevance to the UCPI. Files relating to MoPI group 1 and 2 offences are examined prior to a decision being made to destroy and any decision to destroy must be counter-signed by the Head of Records Management. Once a decision is made to retain a file it will not be reviewed again for destruction for 10 years. Any relevant files identified during RRD review will be flagged to AC-PIT. As of 2016 a new process is being implemented whereby MoPI group 3 files are destroyed after reaching their retention period. In order to prevent automatic destruction of any such files which may be relevant AC-PIT have commenced development of a list of all undercover operations identified which will be cross-referred to RMS records to flag any relevant MoPI group 3 files for retention. I have further determined to flag all file types relevant to units known to have had the capability to deploy the tactic or who regularly use the tactic in more complex

Signed: [redacted] Date: 29th July 2016

investigations/operations. Once flagged files will not be subject to RRD for the duration of the UCPI and will not be released to any individual requesting them without the authority of the Head of Records Management.

I now wish to add as follows in response to the UCPI's request for clarification/further information dated 1 July 2016

88. The UCPI's request refers to the ordinary procedure for document retention referenced at paragraph 14 above and that application of that guidance might lead to destruction of potentially relevant material. I confirm that the MPS (and my own) approach is that while material will continue to be reviewed during the UCPI the default position for all material identified as of potential relevance to the UCPI will be that it be retained. The exception to this is material held in IMOS where a decision has been made to suspend all RRD for the duration of the UCPI. This understanding provides the reason for and justification of all of the steps set out in this witness statement to prevent potentially relevant material being destroyed.

89. The staff responsible for RRD are those in Records Management. Records Management staff make all decisions in relation to RRD of General Registry files. RRD decisions in relation to files held in local archives are made by locally assigned staff who are not specialists in Records Management. These locally assigned staff work to formal RRD processes and instructions, supported by the Op Filesafe team of Records Management specialists. The ways in which Records Management and locally assigned staff have their attention drawn to the requirement not to delete material of potential relevance to the UCPI are those set out above (in particular measures delivering Operation Filesafe which draw specific attention to the requirement to retain potentially relevant information).

90. Following the UCPI's letter of 1 July 2016 I have made enquiries about modifying the guidance referred to at paragraph 14 so that the guidance itself refers to the requirement not to delete potentially relevant material. As a result:

   a. I have been told that the MPS version of the National retention assessment criteria are now in the process of being amended to include words to the effect that if material is of interest to a public inquiry it must not be destroyed.

   b. The MPS is seeking the national version of the National retention assessment criteria to be amended in a similar manner (though the national version is not within MPS control).

   c. The MPS is investigating whether it is possible for the MoPI and/or College of Policing Authorised Professional Practice on information management to be amended in a similar way.

91. With regard to the remainder of paragraph 14, I do not consider that it is a realistic possibility to seek amendment of the Data Protection Act 1998.

92. In relation to preventing abuse of the facility to delete material from INFOS (paragraph 64):

   a. As the possibility of deletion was not known about prior to the work undertaken for the UCPI's request, my belief is that it is extremely unlikely or impossible for abuse to have occurred before this knowledge was gained.

   b. The facility to delete records is only available to an extremely small number of people in SC&O35. This restriction of the deletion facility reduces the risk of abuse as fewer individuals are able to delete records and any deletion is easier to trace.

c. There will be an audit check of user identifications of INFOS every six months to see if any files have been deleted (to lead to appropriate investigation if files have been deleted). This audit will be recorded and the record will be kept.

d. I emphasise that deletion of files from INFOS is not part of a regular process and reiterate that to date SC&O35 are not aware of any deletions having been made at all.

93. In relation to paragraph 77 above and on the issue of prevention of destruction of potentially relevant material by this commercial provider, the service level manager of the provider has informed me that:

a. The system under its control does not operate automatic deletion of records;

b. At present, there are no officers or staff in the MPS with NSPIS access with the capability to delete records;

c. Capita staff with the requisite access rights could delete a record. If they did this they would also delete documents linked to that record.

d. The system is backed up every 24 hours and backups are retained for 12 months. This allows recovery of records if they have been deleted within this timeframe.

e. The provider would always request force approval from NPCC officer level prior to deleting a record and any such request would be routed through the force business support desk.

Signed: [redacted] **Date:** 29th July 2016

f. Application support engineers at the provider are made aware of the need for NPCC level approval before deletion of a record and this approval is recorded in the request on the provider's service toolset.

g. The service level manager has been in that role since 2011 and, in that time, no MPS NSPIS records have been deleted.

94. From the above, my understanding is that no records on NSPIS may be deleted without NPCC level authorisation from the MPS and that there is no routine review and destruction of records. For these reasons and from the information I have been told as stated above I believe that the measures to verify that the instructions sent to MPS officers have been received and acted upon are sufficient to ensure that potentially relevant material is not deleted, particularly as NPCC level officers would require a detailed rationale before authorising a deletion and they have been given specific briefings in relation to the UCPI and the obligations on the MPS.

95. However, as an additional safeguard for the UCPI I have requested the service level manager to inform AC-PIT if the commercial provider is requested to delete a record. AC-PIT will then check to ensure it is not potentially relevant to the UCPI and for any deletion of record(s) to be recorded.

96. In relation to paragraph 93(b) I have asked for a review of the present situation whereby MPS staff or officers do not have the ability to conduct RRD of material on NSPIS.

97. The steps in sub-paragraphs 82(a) and 87(e) do not apply to the commercial provider because:

a. It is not considered to be compatible with MPS security obligations to supply the list proposed at sub-paragraph 82(a) to the commercial provider. The material on NSPIS is not of the sensitivity as that on other systems and the increase in risk that would accompany sharing such a list with the provider is not considered to be justified considering the current position on deletion of NSPIS records as stated at paragraph 93 above.

b. As set out at paragraph 93 above there is no RRD process applied to NSPIS records; the measures described at sub-paragraph 87(e) are not applicable.

Appendix 1. Timeline of delivery of Op FileSafe

May 2014	DSU Hutchison appointed to lead
May 2014	DAC Rodhouse requests Tactical options paper regarding direction from Management board to conduct 'sweep' of all MPS controlled premises for incorrectly filed materials
May/June 2014	DSU Hutchison submits Tac options paper for delivery of FileSafe
June 2014	Information Management Steering Committee briefed on Strategic User requirement for system to enable scanning of corruption archives into digital system
June 2014	AC-PIT commence working with MPS Records Management to

Signed: [redacted] Date: 29th July 2016

	review policy and processes
June 2014	AC-PIT requirements analysis identifies first serious risk to delivery in lack of corporate Information Asset register (IAR). Identified wide range of existing corporate databases with limited consistency and compliance in use, no central search capability and no ability to generate compliance data. Consultation with National archives identifies this as serious risk to delivery of strategic objectives. Digital Policing engaged to provide solution.
June 2014	Briefing paper and tactical plan submitted to AC Hewitt (D770).
June 2014	AC-PIT begin identifying Senior Designated officer for all 443 buildings in MPS estate to lead on 'sweep.'
June 2014	AC-PIT identify second serious risk to delivery. MPS deep storage facility has very limited records of material held other than crime files recorded on RMS. Evidence of very large scale submissions of files to deep storage without effective, searchable records maintained of what submitted.
30 June 14	AC-PIT submit briefing note to AC Hewitt highlighting risk to delivery and resourcing requirements. DSU Hutchison recommends extending time period for delivery of FileSafe to address risk to delivery (D767).
July 14	Information Asset Register High level IT requirements supplied to Digital Policing/Chief Technical Officer
July 14	AC-PIT identify third serious risk to delivery - Shared Support Services provide details of documentary material currently held in local archives. This scoping identifies categories of material filed locally which should be held in General Registry and recorded on RMS
July 14	Digital Policing submit Initial Viability assessment for IAR
July/Aug 14	BOCU appoint SPOCs who are provided guidance from Op FileSafe on reviewing Records management
Aug 14	AC-PIT identify fourth serious risk to delivery. Role of Information Manager on BOCUs is vacant in a number of areas and some

Signed: [redacted]

Date: 29th July 2016

	staff lack skill and training in role
Sept 14	Digital policing major change application considered at CTO steering group. [redacted]
Sept 14	Commencement of FileSafe Steering and Working groups (D765 & 766)
Sept 14	Briefing note on 'Progress on reform of MPS Records Management' submitted to AC Hewitt (D768)
Oct 14	Op FileSafe commence pilot at Croydon BOCU
Oct 14	Op FileSafe strategic plan considered by Independent Scrutiny panel
Oct 14	DSU Hutchison submits scoping and options paper to AC Hewitt re delivery of FileSafe. Papers identify a number of delivery risks and propose options to progress (D763 & D764)
Oct 14	Application submitted to set up Small Projects team within Digital policing to deliver IAR solution
Oct 14	Briefing delivered to all designated Local Service Delivery Managers (LSDM) regarding FileSafe. Includes requirement to retain all material potentially relevant to the UCPI
Nov 14	Op FileSafe review existing MPS Information directory previously developed to provide an IAR for locally archived material. Determined that re-commissioning of this directory was unlikely to meet the identified business need
Nov 14	Following engagement from FileSafe NCTPHQ determined that as MPS have no jurisdiction over the unit they were not required to comply with FileSafe directions but would remain engaged in order to identify and follow best practice (D772)
Nov 14	Presentation delivered to MPS Prosecutions Senior Leadership team including need to identify and retain material relevant to UCPI
Nov 14	Records Management toolkit approved by Commissioner
Nov 14	Digital policing present to Information Management steering committee re progress on high level IAR project. Having

Signed: [redacted] Date: 29th July 2016

	researched five options for an interim solution the only option available for use in the pilot was a locked down Excel spreadsheet. DP reported progressing set up of Small projects team to deliver [redacted]
Dec 14	Op FileSafe commences engagement with Property services team leading on closure of disposed MPS properties
Dec 14	Small projects team approved by Investment board and procurement commences re [redacted]
Dec 14	Croydon pilot identifies that large proportion of files apparently stored in deep storage cannot be found. A significant proportion have been incorrectly archived rather than submitted to General registry. Policy decision made to retain GR material for 1 year on BOCU before submission to avoid swamping GR. Further policy decision to retain other local archive material for maximum of 2 years on Borough before submitting to deep storage
Dec 14	Communications plan for roll out developed with Internal communications yet. Internal comms
Jan 15	Communications strategy developed to be rolled out across BOCUs. Includes need to flag up any identified UC material to Op Beacon and proforma to submit in relation to material identified
Jan 15	FileSafe creates a scoping and options paper in relation to identified risk in relation to MPS deep storage facility. Paper recommends engagement of Agency staff to conduct review of material, identify lost files, destroy when appropriate and develop an accurate and populate Information asset register
Jan 15	FileSafe agree with Property services that rollout will prioritise buildings scheduled for disposal. This is a less efficient and more high risk strategy than roll out on a territorial BOCU basis as planned. However business planning to achieve cuts to MPS budget is likely to lead to disposal of majority of current MPS real estate over the next few years. These premises need to be prioritised to clear them for disposal and ensure material not lost

Signed: [redacted] Date: 29th July 2016

	or inappropriately disposed of during the clearing process
Feb 15	FileSafe roll out plan designed to cover all MPS by Mar 2016
Feb/Mar 15	Dedicated FileSafe Intranet site established as one stop location for policy and guidance on new RM processes and implementation of FileSafe. Launched with Intranet article to introduce new Records management process and toolkit. Article in the Job magazine which mentions FileSafe team looking to identify any material relevant to undercover policing. Process wire diagram for material being reviewed contains specific reference to identify undercover related material and report it to FileSafe team
Feb 15	FileSafe identify risk to delivery re capacity of Met prosecutions and SSS to process material. Options paper submitted recommending engagement of Agency staff (D788)
Mar 15	Strategic update provided to AC Hewitt (D786). Identifies key risk with files incorrectly stored in local archive rather than General registry (estimated 300,000 files requiring transfer to GR and inputting to RMS)
Mar 15	Roll out plan reviewed following learning. Estimated completion date Feb 17. Decision that all roll out to be supported by dedicated RM team will delay completion but maintain QA and enable training
Apr 15	Op FileSafe present business case recommending NCALT_014_02_00 NCALT (Lawful Handling of Information) and NCALT_056_02_00 (MoPI Module 2&3: Collection and Recording) packages to be made mandatory for all staff. Estimated opportunity cost to organisation in excess of £2 million (D787)
Apr 15	Op FileSafe internal Communications strategy updated (D771)
June 15	E mail to all Chief Officer Groups, Borough and OCU Commanders, Area Service Delivery Managers and Local Service Delivery Managers regarding emerging problem with backlog of non-charged volume crime files due to LSDM teams having insufficient resources to cope with workload handed over from Met

Signed: [redacted] Date: 29th July 2016

	Prosecutions
June 15	Digital Policing report have cancelled [redacted] and Small projects team projects. Insufficient resources to progress at present due to need to service higher priority projects
June 15	PSD requested to provide overflow site to cope with storage of material located via FileSafe and submitted to GR
June 15	Digital Policing propose scoping [redacted] as a more suitable solution to IAR requirement
July 15	Submission of Risk and blockages paper in relation to FileSafe to AC Hewitt
July 15	Submission of resources paper to Management board requesting dedicated team and budget to support the UCPI. Paper requests £750,000 funding for Agency staff to support roll out of Op FileSafe
July 15	Briefing note submitted to AC Hewitt re progress in relation to tackling criticisms of MPS Records management made in SLIR (D759)
July 15	Management board agree allocation of £500,000 from Major change fund for Agency staff to support RM team in delivery of FileSafe
Aug 15	AC-PIT complete spreadsheet on current MPS IT corporate and non-corporate systems (565) and identify those IT systems and paper archives likely to contain material potentially relevant to the UCPI (88).
Oct 15	RM team complete review of security arrangements at MPS deep storage facility
Dec 15	6 Agency staff join Records Management FileSafe delivery team funded by £500,000 allocated in July 15

Signed: [redacted] **Date:** 29th July 2016

Appendix 2: Operation FileSafe progress report to December 2015

D773 refers:

To date under Op FileSafe 159,909 paper records have been reviewed:

- Approx 500 missing registry files have been recovered to date.
- 112,454 records have been sent to TNT [redacted] for deep storage.
- 39,602 have been reviewed and destroyed in line with RRD policy
- 7,853 records have been added to RMS in the last month.
- 32,000 misfiled serious crime files requiring registration have been identified.
- From January 2016, all records will be recorded on RMS due to inability of Digital Policing to deliver an Interim Asset Register. All records recorded on spreadsheets will be re-keyed onto RMS.
- In November, 37,000 Camden & Islington logged records were sent to TNT from the Op FileSafe holding archive in [redacted]
- As part of the NSY closure programme, senior officer private offices based at NSY have commenced the transfer of confidential records to - TNT [redacted]
- To improve the quality and quantity of properly registered files, we are working with SC&O and Met Prosecutions teams to train them in RMS input. To date we have **trained 173** additional officers and staff.
- We have now cleared 32 local archives
- SCO4, SCO8, SO20, Merton, Newham, Barnet, Kensington & Chelsea, Hammersmith & Fulham BOCUs are all currently engaged with archive clearing.
- Work continues at Corporate real estate exiting and receiving sites including NSY and ESB.
- In November, 84 records were returned to the National Archives. Plans are in place to transfer a further 1,000 records currently held at Hendon.
- A meeting was held with SCO5 to ensure that historic GN88 (older child abuse/non-accidental injuries records) are properly managed under revised governance to meet additional requirements arising from the Goddard Inquiry. A follow up consolidation is scheduled for December.

1. An additional six fixed term staff joined the delivery team in December following allocation of funding in July 15. This will enable the project to get back on track for scheduled completion by March 2017. From current experience we expect to manage over 6 million records between now and

March 2017. Better processes and direct support from devolved responsibility to officers and staff will allow us to achieve the targets.

2. The primary goal of a sweep of the entire estate and the proper logging and archiving of all material requiring registration will be met. In addition we expect to deliver significant improvements in the management of all MPS records and our alignment to MoPI standards.

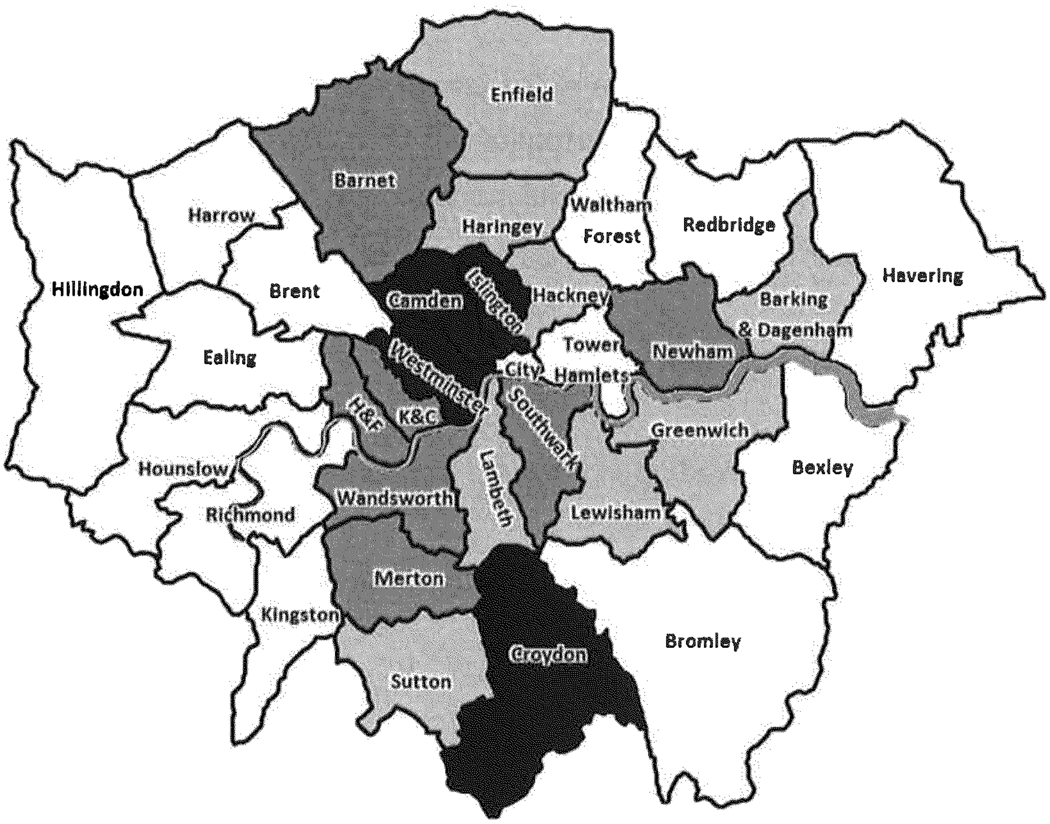
Mapped FileSafe Intervention @ Nov '15

Note: All specialist OCUs are picked up in Borough location activity. The programme is prioritised by CRE building closures

Not started
Engaged
Underway
Nearing completion
Completed

Signed: [redacted]

Date: 29th July 2016


Enfield
Barnet
Harrow
Haringey
Waltham Forest
Redbridge
Havering
Hillingdon
Brent
Camden
Islington
Hackney
Barking & Dagenham
Ealing
Westminster
Tower Hamlets
Newham
City
H&F
K&C
Southwark
Greenwich
Hounslow
Lambeth
Bexley
Wandsworth
Richmond
Lewisham
Merton
Kingston
Bromley
Croydon
Sutton

Signed: ______________________________ **Date:** ______________________