

1. Introduction

The Counter Terrorism (CT) Command SO15 is responsible for countering the threat from Terrorism and Domestic Extremism on behalf of the MPS. In addition to its current information collection, it has also inherited large volumes of information from the Anti-Terrorist Branch and Special Branch, incorporating records from SO1 areas of responsibility. The paper copies of these legacy data sets present a problem in relation to storage. The electronic copies of historical data undermine the effectiveness of our IT systems and adds to the expense of new technical solutions.

This briefing note highlights some risks in terms of both intelligence and legal failure and suggests a number of mitigation measures. The note describes a dilemma caused by competing requirements.

The competing needs are as follows:

1. Operational access to historic intelligence.
2. Compliance with Data Protection Act, Management of Police Information, the Public Records Act and MPS reco
3. Providing access for purposes of public accountability to Public Enquiry Team, Operation Herne, other DPS enquiries, high profile sexual offender enquiries (Operation Midland etc)
4. To reduce reduces risks posed by the decant of SO15 from NSY as office space is at premium.
5. To reduces the information storage burden on our IT systems.


Several recommendations are made but because of the need to provide information to the public enquiry team and Operation Herne, I suggest that the competent decision making authority for any destruction decisions sits outside of SO15, if not outside of SO. AC Hewitt has oversight of Operation Herne, the related Public Enquiry and the MPS Information Assurance and Security Board.

Summary of recommendations:

- That subject to a requirement to retain material for a genuine policing purpose, material in SO15 which is older than 15 years is considered for deletion.
- That the default position will be to delete once material is 15 years old unless required for :
 - Unsolved CT/ DE investigations.
 - CPIA purposes.
 - Post conviction appeal.
 - High profile external enquiries (public enquiry, Herne etc).
 - Required to be kept by legislation or other statutory purpose
- This policy will apply to hard copy data, electronic files or data and physical exhibits.

Specialist Operations MANAGEMENT OF INFORMATION WITHIN SO15

Version 1.0

Title	Name	Signature (Hard Copy Only)	Date
Author	 (NCTP HQ) BAND A1		11th June 2015.
Supported by			
(OCU Commander)	Commander Richard Walton		19th June 2015

1. Introduction

The Counter Terrorism (CT) Command SO15 is responsible for countering the threat from Terrorism and Domestic Extremism on behalf of the MPS. In addition to its current information collection, it has also inherited large volumes of information from the Anti-Terrorist Branch and Special Branch, incorporating records from SO1 areas of responsibility. The paper copies of these legacy data sets present a problem in relation to storage. The electronic copies of historical data undermine the effectiveness of our IT systems and adds to the expense of new technical solutions.

This briefing note highlights some risks in terms of both intelligence and legal failure and suggests a number of mitigation measures. The note describes a dilemma caused by competing requirements.

The competing needs are as follows:

1. Operational access to historic intelligence.
2. Compliance with Data Protection Act, Management of Police Information, the Public Records Act and MPS reco
3. Providing access for purposes of public accountability to Public Enquiry Team, Operation Herne, other DPS enquiries, high profile sexual offender enquiries (Operation Midland etc)
4. To reduce reduces risks posed by the decant of SO15 from NSY as office space is at premium.
5. To reduces the information storage burden on our IT systems.

Several recommendations are made but because of the need to provide information to the public enquiry team and Operation Herne, I suggest that the competent decision making authority for any destruction decisions sits outside of SO15, if not outside of SO. AC Hewitt has oversight of Operation Herne, the related Public Enquiry and the MPS Information Assurance and Security Board.

Summary of recommendations:

- That subject to a requirement to retain material for a genuine policing purpose, material in SO15 which is older than 15 years is considered for deletion.
- That the default position will be to delete once material is 15 years old unless required for :
 - Unsolved CT/ DE investigations.
 - CPIA purposes.
 - Post conviction appeal.
 - High profile external enquiries (public enquiry, Herne etc).
 - Required to be kept by legislation or other statutory purpose
- This policy will apply to hard copy data, electronic files or data and physical exhibits.

2. Background and Business drivers.

The Counter Terrorism Command collects a wide range of information in order to carry out its core business. This information has been stored within a number of different systems both in digital and hard copy archives.

Like the rest of the MPS, the Counter Terrorism Command (SO15) has not have been diligent in its application of the MPS Review Retention and Disposal Policy (RRD) for the information it holds. This lack of compliance generates significant legal risks for the organisation and overcomplicates IT requirements.

Within SO15 the lack of compliance has generated additional risks as evidenced by recent criticism by Chief Constable Creedon (Operation Herne) and others.

Legal risks include lack of adherence to the Data Protection Act 1984 (DPA) and the Information Commissioner could take enforcement action against the MPS. Such action would result in adverse publicity and potentially a large financial penalty.

There is increasing pressure on accommodation and storage space is likely to be at a premium. Storage off site through Records Management branch is costly

The purpose of this report is to highlight the nature and scale of the problem and scale and propose several solutions.

SO15 has established a review team as part of the preparation for the roll out of the [REDACTED] IT system but that will only address the RRD risk for one part of the catalogue of data sets held within SO15, namely records on NSBIS (National Special Branch Intelligence System) along with hard copy files retained in IMOS (SO15 hard Intelligence record archives).

The MPS version of NSBIS and the historic files held within IMOS, in addition to holding material of long term operational interest, hold the material of interest Operation Herne, the Public Enquiry team and others. The establishment of this RRD capability will address the current "Herne related" high risk issues attracting media attention. However this leaves other high volume and increasing data sets, which are not the subject of any systematic current review regime.

In addition to the application of an effective RRD policy, effective information management requires the exploitation of information assets. Some of the SO15 datasets are not being exploited to their maximum potential.

3. Guidance / Legislation.

Best practice under the MOPI guidelines (Management of Police Information) would include recording of:

- retention grounds
- retention period when first assessed
- review period for the material to assess if the retention grounds remain valid.

The MPS has a robust and refreshed Information Management policy which reflects those principles. Most of the intelligence and operational information held within SO15 would fall into a category of Serious Specified Offences (CJA 2003). In which case the MPS, having recorded the policing purpose justifying our decision, can

under the National Retention Assessment Criteria (NRAC) retain such material for 100 years and review on a regular basis (at least within every ten years). MOPI does provide guidance and although MOPI is not legislative it is issued under the authority of the Police Act 2006. The principles of the Data Protection Act 1998 place other legal obligations upon the MPS in relation to the RRD of information. In particular, principle five dictates that personal data should be retained for no longer than is necessary.

Failure to comply with MOPI could undermine public confidence; attract media or political criticism and legal sanctions from the Information Commissioner.

4. Scale of the problem

In addition to data sets held on corporate systems such as Aware and Crimint, SO15 has digitally stored information on several main databases (at up to TOP SECRET) and hard copy file archives.

Attached to this report is a table, marked Appendix A, providing comments about the risk posed by each of several data or information stores controlled by SO15. These are as follows:

- CT Holmes
- IMOS (which is subject to a current PDF scanning project)
- Hi Tech Unit
- Ports Digital Seizures
- Archives in [REDACTED]
- Dedicated Source Unit / Covert Functions Archives
- CLIO on SKY and National CLIO
- S drives on SKY
- NSBIS
- Policy Papers
- AWARE / Foundation / SO15 CRIMINT
- Hard Copy material stored at TNT.
- Exhibits.

5. Consequences and Risks

Lack of application of an effective RRD policy in SO15 has a number of potential consequences:

- Unnecessary pressure on our accommodation as space is needed for storage.
- Enforcement action / prosecution of the MPS by the Information Commissioner involving potential large financial penalties / fines.
- Consequential reduction in public reassurance / public support.
- Unnecessary complication of our IT requirement and systems.
- Unnecessary cost of storage of archived files at TNT.

As can be seen from the table at Appendix A, the risks generally fall into the following categories.

- Intelligence failure
- Inability or reduced ability to comply with legal requirements such as DPA subject access requests of Freedom of Information Act requests .
- Inability to satisfy Public Enquiry Team's / Operation Herne's requirements.
- IT systems which are ineffective and fragile.
- Extra accommodation pressures.

6. Options

There is no immediately obvious strategy which would address all the issues raised in the attached table in **Appendix A**. The staff required to review the legacy material across the different datasets are simply not available.

However we can do something about the material held in IMOS who already have a locally recruited team reviewing, indexing, scanning, and indexing older records. In relation to IMOS the following options should be considered.

1. Authorisation of the deletion of INFOS files once scanned onto the PDF system.

Although the original file would not be available for viewing there would be a searchable retrievable image. Once scanned these files should then be deleted

2. Authorise the destruction of all files which are dated prior to 2000.

The scanning project, at the current back record conversion rates, will have scanned onto the PDF system all files back to 2000 by the expected date of decant from NSY. This does represent an operational risk, but much of the material that would be destroyed is already summarised on the BRS / NSBIS system hence lessening the operational impact. The application of a policy for the destruction of files created before 2000 could impact on current external enquiries including Herne and the public enquiry and alleged allegations concerning Members of Parliament. However it would be DPA and MoPI compliant. The alternative would be to retain part of, or our entire inventory (approximately 45000 files) at TNT or similar. Use of this comes at a significant cost, estimated at approximately £250,000 over a 5 year period for the retention of our inventory in hard copy at TNT [REDACTED] It would also make access to the files very difficult and time consuming.

3. If authorised, this solution could be applied to other data holdings i.e. delete material that was generated prior to 2000 including other hard copy archives.

4. In relation to the other datasets mentioned above and in Appendix A. The scale of the problem is not going to improve without significant work and resources. We might be able to consider a deletion policy along the lines of the material in IMOS but that requires a more operationally driven assessment of the risk.

5. It is recommended that the Command appoint a lead for each of the datasets who should be tasked to make an assessment of the operational risks generated by such a proactive deletion policy

Governance

Once a policy has been agreed then we need to insure that it continues to be applied in the future. This could be one of the routine inspection themes of NCTPHQ who will report into each OCU Commander via the Lead for Compliance and Assurance.

Submitted for consideration

[REDACTED]

BAND A1

NCTP HQ

MPS - UCPI
PROVISIONALLY
REDACTED

RESTRICTED

Appendix A to SO15 report dated 11th June 2015 concerning Information Risks in SO15

Database.	Comment	Risks
CT Holmes 17	System has existed for approximately thirty years in various guises. The total number of current and historic operational investigation accounts is [REDACTED] dating back to the early 1990s. In addition an Altia database contains hundreds of gigabytes of scanned documents and exhibits from 2007. Material will contain personal data and although investigations are reviewed, we are not applying any significant review process for the purposes of RRD / MoPI / DPA.	No RRD policy. Lack of DPA compliance Intelligence gaps. System resilience due to volume of material
18	[REDACTED]	
IMOS	This is an intelligence file library sitting on the [REDACTED] containing approximately 80,000 files which were created as the hard copy database for Special Branch record system. Further Details concerning IMOS are contained at the bottom of this table.	RRD policy has historically not been applied. Files required for Operation Herne and Public Enquiry. Significant accommodation pressure. Files sometimes for consultation for current intelligence purposes.
High Tech Unit	This unit collects analyses and stores the digital material obtained from operational activity. E.g. all digital material obtained from suspects' mobile phones, laptops, tablets and personal computers. These contain personal data as defined by the Data Protection Act 1998. The volume of material held is growing at a significant rate and it may now amount to almost one and half Petabytes (1000 Megabytes = 1 Gigabyte, 1000 Gigabytes = 1 Terabyte, 1000 Terabytes = 1 Petabyte). We are not applying an effective Management Information Policy or RRD policy in relation to this material.	No RRD policy. Not searchable [REDACTED] Not searchable [REDACTED] System resilience due to volume of material
20	[REDACTED]	

19

RESTRICTED

	[REDACTED]	
<p>Ports Seizures</p> <p>Digital</p> <p>21</p> <p>22</p>	<p>Persons are examined at Ports through powers granted by Schedule 7 of the Terrorism Act 2000, officers are empowered to seize and examine any material with that person. Frequently all digital media carried by that person (phone, tablet, laptop etc) is copied using the [REDACTED] and sent to the Hi Tech Unit and also retained on the Sky IT system. It is frequently copied to the National Ports Analysis Centre. This digital data contains large amounts of personal data of the person examined and others. <i>Legal advice obtained by office of National Coordinator Prevent and Prepare suggests that responsibility for the RRD of this data rests with the originating collecting Force.</i></p> <p>I can find no evidence of any systematic process for the review of material collected under Schedule 7 powers.</p> <p>Similarly the "Ports data store sits in isolation from the other Intelligence databases. [REDACTED]</p>	<p>No RRD policy.</p> <p>Not searchable [REDACTED]</p> <p>Not searchable [REDACTED]</p> <p>System resilience due to volume of material</p>
<p>Archives in [REDACTED]</p> <p>24</p>	<p>The SO15 units at [REDACTED] are responsible for a number of file stores of sensitive material [REDACTED]. There is also a large volume of material relating to Irish Republic Terrorism which has special handling restrictions. In the main this is indexed on a separate closed version of the SKY IT system [REDACTED]. These documents and electronic records frequently emanate from, or contain material from, the Security and Intelligence Agencies. There are no systematic processes in place for the application of an RRD policy for this material.</p>	<p>No RRD policy, therefore not MoPI compliant</p> <p>Takes up valuable accommodation space.</p>
<p>Dedicated Source Unit / Covert Functions Archives</p> <p>25</p>	<p>This contains approximately [REDACTED] physical files relating to CHIS activity by SO15 and SO12 dating from the 1970's to present day. Although some of the files are indexed in a protected manner on SKY, it is only the subject's name that was indexed. Details of tasking, other bio details, intelligence generated (although disseminated at the time) is not searchable within that physical data. A succession of decisions about the deletion of CHIS records have been made by the National Source Working Group and MPS Directors of Intelligence / Covert Policing. The current position is that CHIS records are rarely deleted. A project was initiated to</p>	<p>No RRD policy.</p> <p>Intelligence gaps.</p> <p>System resilience due to volume of material.</p> <p>Accommodation Pressures.</p> <p>Not searchable [REDACTED]</p> <p>23</p>

23

RESTRICTED

	identify a means of making this archive more searchable, no solution has yet been identified and there is no current RRD activity taking place.	
CLIO on SKY and National CLIO	Proactive CT and DE Operations Room run from the CTPOR (Ops Control Room), use the CLIO database for the operations management. Operations generate large amounts of data, often personal data, which is stored on the CLIO system, historically on the MPS SKY system more recently on the national CLIO system on TACIT. The size of this data set is not known but since March 2007 we have had 294 separate operations on SKY Clío. These currently show a total of 373190 entries or records .There has been no RRD policy in place for material held on CLIO. Although much material generated is extracted from CLIO it appears that it is often stored into Operational Files in Secure S drives on SKY rather than onto the CT database NSBIS. Exploitation of this information asset will be maximized if the information is placed onto the searchable corporately available database.	No RRD policy. Not searchable outside of the Ops room staff. System resilience due to volume of material. Not searchable Not searchable
S drives on SKY	The Command has amassed a number of reports on operational or team S drives on SKY. Many of these records have been generated by the CTPOR so could be duplicated from CLIO. However many users use them to house sensitive reports. The ability to search within the folders in the S drives is limited to the nominated specific team members only and there is no RRD policy in place. The size of this unstructured database is considerable but our best guess is that it contains 2.2m files or 1.4Terrabytes of data and at least 600,000 files need reviewing. There has been no RRD policy in place for material held within the S drives. (See CLIO about exploitation of this data set).	Not searchable Not searchable Volume undermining effectiveness of SKY
NSBIS	<u>NSBIS</u> This system contains all intelligence reports received into the London Intelligence Unit since December 2011 when NSBIS was adopted. When the system is interrogated to establish how many reports it contains the database is so large, the document search fails - 4,000 reports were added in July 2014 and we've had the system since December 2011. In addition all the data from the preceding system BRS is also stored in the database. Analysis of audit figures gives a best guess suggesting there are approximately 800,000 identifiable records. However, Detective Superintendent Jayne Cowell established an RRD team to commence work on reviewing NSBIS and old files within IMOS that are effectively	RRD policy needs high level approval. No deletion taking place due to the public accountability requirement. System resilience due to volume of material.

26

26

RESTRICTED

	indexed on NSBIS. Although NSBIS is our current intelligence system IMOS / BRS/ NBIS contain the historical records relevant to the current public enquiry and Operation Herne.	
Policy Papers	Until approximately five or six years ago SO15 would frequently archive internal policy papers within IMOS along with Gold Group minutes. This stopped after the OPIC review and each unit has its own arrangement. Many papers are internally registered on a correspondence register within SO15 by Staff Officers but there is no systematic policy for RRD.	Lack of effective tracking. Storage requirement. Long term retrieval. Not easily searchable for FoIA purposes.
<u>Hard Copy material stored at TNT</u>	Management Records Department have not yet been able to establish how much material each OCU including SO15, have stored at the TNT store. The volume is significant. There has been no RRD policy in place for material held at TNT. With time we will be able to establish how much material SO15 have stored at the TNT store.	No RRD policy. [REDACTED] System resilience due to volume of material. Cost is significant. (Note : In respect of the 5449 IMOS files at TNT, it will cost approximately £25,000 to retrieve these files from [REDACTED] Destruction on site without scanning is an option. To comply with provisions of the Public Records Act, files held at TNT require review after 10 years. January 2015 will see 30 boxes being returned at a cost of £3,750 each way to enable this review to be undertaken.
AWARE/ Foundation/ SO15 CRIMINT	We have not been able to establish how much material is saved on the S drives of Aware, it should be non operational material but still needs to be scrutinized in relation to RRD. There is a large volume of SO15 operational material saved into the CRIMINT data base. I am unaware of any systematic RRD activity in relation to SO15 Crimint. There are folders marked SO13 containing operational records on Aware and a recently discovered "SO15 I drive" which is still in use.	No RRD policy. [REDACTED] S drives and I drives not searchable outside of the nominated small number of staff. [REDACTED] System resilience due to volume of material.
Exhibits	At the Exhibits store [REDACTED] SO15 has large storage facilities containing original exhibits which have been amassed over thirty years. Although the MPS has a policy for the disposal of exhibits, the Command does retain material for a considerable length of time	Storage space and cost is considerable.

27

27

RESTRICTED

IMOS.

Background Points.

- **60,000 - 75,000** Secret Pink files dated 1983 - 2011 are held on the [REDACTED]. These cover all CT/DE activity from this period. We are currently scanning these files onto a secure hard drive which will provide searchable pdf copies. Files of interest to Op Herne, Operation Midland and many current politically high profile matters contained in this file library.
- **5449** Secret and Confidential files (in 193 boxes) dated 1930 - 1983 are currently stored at TNT [REDACTED]. These files have not been scanned. The cost of storing these items is now the responsibility of SO15. To return 1 box now costs the Command £125 each way. In total 70 of these boxes have now been returned for Herne/Shay/Irish matters. We have not returned these to save costs, however we are still paying a storage fee even though they are in NSY. Preferred option is to provide Op Herne with a list of files at TNT. A bulk return is made of required files which are then scanned and destroyed. Remaining files destroyed by and at TNT. Second option to return and scan all 5449 files and then destroy.
- **607** SO1 Protection files (in 124 boxes) 1983-2005 are held on the [REDACTED]. Preferred option to pass to Op Midland team or SO1.
- **4** crates of Special Branch records/registers and Irish/Communist material from the 1920's are held on the 19th floor. To be destroyed asap.
- **19** Blue Crates with a numbered seal containing ICS material (Applications for Communications Data) are held on the [REDACTED]. To be offered to op Herne and then destroyed.
- **1358** files from 1936 - 1980 that have been reviewed but not taken by the National Archive are held on the [REDACTED]. To be destroyed. The National Archive only deemed 10% of this 1358 to be of national interest. Remainder assessed under previous RRD policy as not of a current policing purpose. Second option to scan and destroy, which may be more effective then destroying and weeding electronically from NSBIS.
- **322** Nationality Files dated 1953 - 2010 are held on the [REDACTED]. To be returned to Home Office if original Home Office files. If copies, to be destroyed.
- **1300** files of Secret Green / TS Green files held on the [REDACTED]. Bespoke audit and weeding process. If necessary to keep, able to scan and secure on Zamzor IC Desk (TS).

Actions already being taken. Issues or Options to be considered.

- Require a decision and authority to destroy once scanned on to the PDF system.
- Due to the requirements of Herne no destruction has taken place for a significant period.

Changes to the Public Records Act will result in the 30 year rule being reduced to 20 years. This will effectively require all SO15 files to be reviewed by their 15th year and a decision made as to whether to retain or dispose. This legislation applies to files created before 2000. MoPI covers retention of files created after this date.

IMOS began scanning files onto a searchable hard drive in 2013. To date over 9,000 files have been scanned covering the period from 2011, when we ceased creating hard copy, to 2005. There are approximately 10,000 more files covering the period 2000 - 2005. This laborious and costly process using agency staff scans approximately 100-150 files per week. As the files get older, paper quality and print levels deteriorate resulting in photo-copying and darkening of type to allow a successful scan. It is expected that by April 2016 to the team will have created electronic copies of all files from year 2000 onwards at a cost of nearly £80,000 in 2015 alone for agency and permanent staff costs assigned to this task.

Approximately 45,000 other files will remain unscanned and an inventory of these is listed below.

The current preferred option for the IMOS management is relatively simple and is legally/policy compliant and cost effective. A 12month notice period is publicised MPS wide advising that from 01/01/2016 hard copy paper files created pre 2000 will be destroyed in line with RRD policy unless they serve a current policing

RESTRICTED

		<p><i>purpose. Authority of a DSU will be required for a file from this period to be scanned onto our searchable database if required to prevent that becoming the default option for all. The destruction of these files will then take place allowing our decant from NSY. The Command is then left with a searchable record of files covering 2000 - 2011, as well as copies of other files deemed relevant under the RRD policy.</i></p>

MPS - UCPI
PROVISIONALLY
REDACTED