

Pyemont Ellie - Public Inquiry Team

From: Hutchison Neil - Public Inquiry Team
Sent: 22 January 2016 21:44
To: DI Mailbox - DPS Public Inquiry Team
Subject: FileSafe update

Neil Hutchison

Neil Hutchison | Detective Superintendent

Metphone [REDACTED] Telephone [REDACTED] Mobile [REDACTED]
E-mail [REDACTED] Address [REDACTED] New Scotland Yard, Broadway,
London, SW1H 0BG

METROPOLITAN POLICE SERVICE

Protective marking: Not protectively marked

From: Burton Jeremy - HQ Directorate of Professional Standards
Sent: 10 September 2014 11:21
To: Hewitt Martin - CommPO
Cc: Taylor Fiona - HQ Directorate of Professional Standards; Hutchison Neil - HQ Directorate of Professional Standards
Subject: FileSafe update

Sir

Apologies as this is too late for formal circulation to today's Diamond Group. Neil and I met on Monday to discuss progress regarding FileSafe. I am now establishing a formal FileSafe Steering Group and Working Group which will report to your Diamond Group. This change is because progress is being made across the organisation and staff are now in place to support us. The attached is an account of activity thus far for your information

Many thks

J



Briefing note for
AC - Records...

Jeremy Burton | Detective Chief Superintendent

AC Professionalism: Public Inquiry Team

Met [REDACTED] | Telephone [REDACTED] | [REDACTED]
Email [REDACTED]
Address Room [REDACTED] New Scotland Yard, The Broadway SW1H 0BG



Briefing Document:

PROTECTIVE MARKING	Restricted	FOIA EXEMPTION	No
SUITABLE FOR PUBLICATION SCHEME	No	DATE CREATED	6th June 2014
TITLE AND VERSION	Operation Beacon - Briefing note re Op Filesafe		
SUMMARY	Progress Update to 6th June 2014		
HANDLING INSTRUCTIONS This document must be handled in accordance with the protective security marking shown at the bottom of the document and should not be disseminated to outside agencies/partners without the consent of the authorising officer & or Director DPS. This FOIA table must not be detached from this Document			

Op Filesafe - Proposal

Requirement

The Stephen Lawrence Independent Review published 6 March 2014 highlights the failure of the MPS to locate documentary records relating to historic corruption enquiries.

Historic intelligence relating to corruption was held on IT systems that are no longer in operation. The degree of any data loss is currently unknown and subject to investigation. Initial scoping has identified around 3,000 crates of corruption related material from the mid 1990s to mid 2000s held in General registry as well as a hardrive containing thousands of further documents. Further material relating to the terms of reference of Op Beacon may be stored elsewhere in the MPS estate. The MPS has clearly retained a huge quantity of corruption material, much of which appears to be comparatively well indexed, nevertheless it will take months to search these files for material relevant to the Lawrence investigation and we are still unsure whether further material is stored elsewhere.

The weaknesses identified in relation to corruption material also apply to wider Records management. Op FileSafe aims to assess all physical records held across MPS estate, improve Improvement management standards, identify opportunities to introduce improved archiving systems and identify any further material relevant to Op Beacon.

Strategy

The two key questions necessary to determine strategy are:

1. What is the nature of the problem?

The MPS does not currently know what material it holds, where it is and when it can locate relevant material to an issue it cannot always be searched in the required time frame. The Operation objectives of FileSafe are to conduct an assessment. It is anticipated that this will then inform a further project to implement improved Records Management from lessons learned and working from a baseline of information provided by Op FileSafe.

2. What resources are available to address the problem?

MB have allocated 20 police staff to work on Records Management for Op Beacon under a Detective

Superintendent. MPS BCUs in addition have police staff responsible for Records management who can be utilised to assist Op FileSafe. No budget has been granted for Op FileSafe to address issues uncovered as this is an assessment exercise from which further work will be generated to implement digitising and archiving solutions.

Tactics

Leadership and Governance structure

First governance meeting took place on 12th May 2014 chaired by DAC Rodhouse. Set initial objectives:

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

- Do the MPS need to retain the material?
- If so then is it appropriate to be held locally?
- Is there adequate indexing of the locally held data and is there sufficient corporate knowledge of its content and presence?
- Should the data be held in corporate archives?

To assess opportunities to utilise scanning and automated indexing solutions to reduce the volume of material held in corporate archives.

To assess whether any material located as a result of Op FileSafe has relevance to any of the terms of reference for Operation Beacon.

Information management is one of MPS Total Technology programmes and includes Enterprise Content Management reviewing management of paper and electronic records. The Information Management Steering Committee under DAC De Brunner and Digital Policing command under CS Tony Dawson will be key stakeholder in Op FileSafe. Success of Op FileSafe requires integration with these stakeholders as it is clear that sustainable improvement to MPS Records Management will be reliant on delivery of Digital Policing. The Op FileSafe estate sweep is an opportunity to generate quality Metadata to facilitate Digital Policing. Op Beacon's Corruption review provides an operational demand for which Digital Policing will provide the IT solution.

The Digital Policing project aims to integrate all MPS IT systems over the next three to four years to achieve a position where all digitally recorded information is saved on a cloud and therefore, to all intents, in perpetuity. A key success factor for this project will be ensuring that material currently held in bulk storage in hard copy form is appropriately assessed. This will enable consideration as to whether it is suitable for destruction, retaining in hard copy or scanning and uploading into digital form. The Digital Policing team require a product owner for the programme. Following an initial scoping meeting with Ch Supt Tony Dawson it is proposed that Op Beacon Corruption Review team become operational lead for Digital Policing in order that the Corruption review element of Op Beacon can be used to ensure proposed technology solutions meet operational needs of policing.

Recommendation 1 - Establish Gold group chaired by AC Hewitt (Gold), DCS Burton (Silver) and including DSU 1 [REDACTED] (Bronze), Adrian Buckingham (Logistics Director/Shared Support Services), CS Tony Dawson or Mark Welton (Digital Policing), Records Management (to be confirmed), PSD (to be confirmed).

Establish Working group chaired by DSU [REDACTED] including BCU Cmdr representative, Fedrep, Staff association rep, [REDACTED] (DMC), Records Management rep, Shared Support Services rep, [REDACTED] (Digital Policing). BAND B7 DSU 1 BAND C5

Recommendation 2 - Op FileSafe to link in to Information Management Programme led by DAC De Brunner.

Recommendation 3 - Appoint independent External Assurance provider to audit operation.

Assessment of all physical records held in MPS

In order to make this assessment the following actions must be completed:

1. Identify all physical storage locations used/controlled by MPS.

2. Assess all physical records held. This scale of this task requires a scoping exercise before undertaking independent searches. This scoping exercise will risk assess storage locations and material and thereby narrow down material into scales of assessment. As an example of why this is necessary the Digital Policing team estimate that registry alone currently stores in the region of 500 million "documents", each document being an A4 size sheet or equivalent. If the 20 staff allocated to Op Beacon by MB (but not yet recruited) were deployed to actually examine each of the documents in registry alone they would need to examine 22,727,000 each. Digital Policing have no current estimate available as to how many documents are held on BCUs and there is a lack of consistency

across the MPS regarding local filing arrangements. However it can reasonably be estimated that millions more documents are currently FOD. A search/sweep exercise to scan all of this material by eye would not be a cost/effective undertaking given that the large majority is likely to be appropriately stored material, of no relevance to Op Beacon and inappropriate for scanning and digital storage.

3. Protocols exist with MPS Records Management around conducting sweeps of estate buildings. An independently conducted search of a police premises can be more effectively be conducted through providing the search team with a briefing covering the layout of the building and the B/OCUs own metadata assessment of what material is held within. The search team can then compare the B/OCUs record with what they find and thus quality assure the B/OCUs work and identify when they have uncovered material that the B/OCUs have not recorded. POLSA/TSG search of entire estate is not feasible in terms of timescale, cost or availability of appropriately trained search officers. Therefore this scaled approach is recommended dependent on risk evaluation of different premises.

4. The premises assessed as most likely to contain Op Beacon relevant material are likely to be secure/strapped environments such as DPS, SO15 premises. Such premises are likely to require a bespoke plan for material to be reviewed without compromising operational security.

Recommendation 3 - A Concept of Operations is required with Strategic and Practitioner input. It is recommended that private sector record management consultants be engaged in this process. MPS is currently working with both PWC and Cap Gemini, consideration as to appropriate tendering process is required.

Recommendation 4 - Assign an SLT SPOC on each BCU to conduct an initial scoping exercise to identify all premises controlled, all document storage locations within the BCU and what data is currently available on what is held within location. SPOCs will require guidance on generation of Metadata to enable subsequent assessment of material.

Recommendation 5 - Op Beacon team will not have sufficient resources to conduct detailed assessments of premises/archives to assess whether material is of relevance to Beacon. BCUs are to be provided guidance on terms of reference for Op Beacon and an escalation process agreed by which they can refer any material potentially of interest to the Beacon team. The Beacon team will not accept referrals of archives or crates but only of specific files/documents. Should relevant material be recovered Op Beacon may direct a more detailed search of the relevant building by POLSA/TSG advised by Op Beacon staff.

Recommendation 6 - Working group to agree protocol for amnesty for officers/staff to ensure material is located and appropriately assessed and filed. Lack of an amnesty will generate a risk of material being destroyed or hidden to avoid criticism/discipline when it is located.

Opportunities for scanning and automated indexing solutions

The Op Beacon team have held initial scoping meeting with PWC Consultants and Digital Policing OCU on scanning/indexing solutions to digitally store corruption material held in archives and a standalone hard drive. A range of commercial solutions are available some of which can provide a faster, more cost effective and equally secure solution than recording on Holmes and will provide appropriate levels of search and recovery reliability. Digital Policing are engaged in a scoping exercise regarding the range of records management products available on the market. Some of these are storage tools which reduce paper records to a digital format while others scan material into a server in a format whereby it is searchable using Optical Scan recognition (OCR) and Entity Resolution. It is not anticipated that the majority of material identified through Op FileSafe will require to be digitised into a searchable format and it will not be cost effective to do so. However there will be archives identified with clear operational benefits to storing in a digital format which enables search engines to be used. The corruption material relevant to Op Beacon is one example but it can be anticipated that Op FileSafe will identify further such material. Experience of Op Herne indicates that an alternative operation to transfer the corruption material to a Holmes account would take several years and the MPS will struggle to supply appropriately MIR trained staff to undertake this work.

Recommendation 7 - Review initial objective set to use scanning and automated indexing to reduce volume of material held. Scanning should not be considered as simply a storage option. There are various Scanning/indexing systems available and Op FileSafe provides an opportunity to identify archive material where direct operational benefit will be gained from digitizing in a format that enables OCR and Entity Resolution e.g. corruption archives can be made available in searchable format to existing DPS Intelligence database.

To assess whether any material located as a result of Op FileSafe has relevance to any of the terms of reference for Operation Beacon

Op FileSafe will prioritise assessing stored material to determine if it is of relevance to Op Beacon

Op Beacon material can be widely identified as material relating to Corruption investigation, Lawrence investigation, SDS operations and Undercover policing. While the initial Op Beacon proposal focuses on corruption material from 1994-2008 this is too restrictive a time period for consideration of potentially relevant material. Continuing uncertainty regarding the ToR of the upcoming Public Inquiry generates the possibility that any material relating to investigations/intelligence operations involving Undercover officers could be relevant to Op Beacon. Loss of such material could make it more difficult to defend appeals against convictions or civil claims relating to cases where an involvement of an undercover officer is alleged.

The time scales and resource implications of assessing material must not be underestimated. Example 1 - SO15 DSU at [REDACTED] has been assessed as a location with a high likelihood of holding material relevant to Op Beacon/Herne. Material is currently held in hard copy and is not filed and indexed in a searchable format. An initial scoping meeting has been held which suggests review and indexing will take SO15 DSU approximately 6 months. Operational security requirements prevent use of external staff to conduct this work. Example 2 - Review of SDS records held within SO15 IMOS for Op Herne/Elison review to identify all material with potential relevance to Lawrence investigation/inquiry took vetted staff from both SO15 and Op Herne several weeks to complete.

An immediate instruction to all MPS B/OCUs to review all filed material to identify any material relevant to Op Beacon is likely to result in negative responses which would not stand up to any scrutiny regarding the thoroughness of the review, as occurred with the May 2012 report.

Costs and Resources

Capacity to advise and support B/OCUs through the process will be dependent on identification and recruitment of dedicated staff. MB have authorized deployment of 20 Band Ds and 1 Band C to assist Op Beacon in relation to Records Management. It is anticipated that these staff will be used to review existing MOPI guidelines, consolidate what Metadata is currently held, provide a Standard Operating Procedure for BCUs to implement, provide a central point of advice and support to B/OCUs and provide an Internal Assurance provider capability. A process of identification and recruitment of these staff is required to ensure appropriate resources available. At present Op Beacon does not have a BWT or dedicated budget line. The Concept of Operations requires clarity regarding what budget is available to employ private sector consultants to advise and provide digital storage solutions and what budget line can be bid into by B/OCUs/SSS to arrange transport, storage or destruction of material which is assessed as no longer suitable for local storage. Existing Tasking budget is not sufficient or suitable for bids or to arrange POLSA/TSG sweep of estate where necessary.

Initial review of existing storage facilities indicates that registry at [REDACTED] is already operating at 110% of capacity. Op FileSafe is likely to reveal that some BCU archive/storage facilities are not fit for purpose and require building works or transfer to alternative locations. Example - FOD store at [REDACTED] BCU has a leaking roof that has resulted in damage to material. Repeated requests to PSD have not achieved a permanent repair of the leak.

Material identified as suitable for transfer to corporate archives/TNT storage will generate further costs for indexing, transport and storage.

Recommendation 8 - Op Beacon resource bid agreed by MB on 7th May to become formal establishment. Costs currently assessed as staffing only. Budget line is also required for costs of Op FileSafe. Size of this budget to be considered as element of Concept of Operations. Estimate of cost of private sector digital storage solutions requires tendering process.

Recommendation 9 - MPS Records management to begin scoping of additional storage facility ready to cope with likely large increase in material being sent to registry as BCUs review held material.

Recommendation 10 - Op FileSafe to provide a Intranet accessible guidance document and Q and A facility to assist BCUs in conducting Op FileSafe and ensuring ongoing MOPI compliant local records management standards.

Prevention of material being destroyed/lost prior to recovery under Op FileSafe

MPS operates under MOPI guidelines which are nationally agreed protocols. The risk of material relevant to Op Beacon being inappropriately disposed of prior to Op FileSafe locating it is mitigated by the lengthy retention periods for serious crime (up to 100 years) and Intelligence (up to 100 years depending on severity of crime to which linked). Op Beacon assess that under current guidelines corruption material relating to crime will be retained for a minimum period of 12 years. Delay in implementing Op FileSafe is unlikely to result in loss of material relevant to Op Beacon. Direction to B/OCUs to assess all material held without providing appropriate guidance, support, amnesty arrangement and local and corporate risk and control measures may result in material being hidden or destroyed to avoid reporting/assessing it. A further risk exists of false assurances being given by BCUs that they

have adequately reviewed material resulting in further risk to the MPS. Should the task have to be repeated due to it being inadequately conducted at the first attempt this will waste staff time and increase the likelihood of inadequate reviews being conducted by B/OCUs.

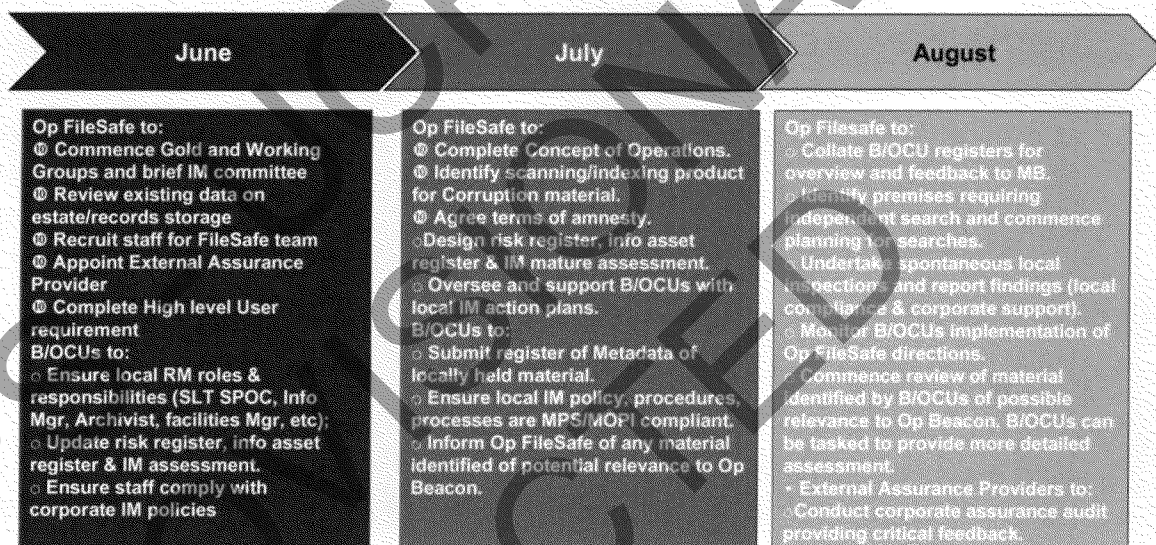
Recommendation 11 - Op FileSafe prepare guidance document for B/OCUs regarding what material needs to be retained in original paper form even after having been digitized for reasons of evidential continuity and with MOPI compliant guidelines for retention.

Recommendation 12 - A realistic timescale for Op FileSafe is 12 months. Implementation of estate sweep prior to some other aspects of the operation being put in place could increase risk of material being lost.

Three lines of defence model

The three lines of defence model will be used to construct layers of responsibility and oversight. An initial draft for Op FileSafe has been prepared by the Head of Records Management which has been used to propose the following proposal for progress over the next three months.

Immediate Timescales



Submitted for your information,

Detective Superintendent Neil Hutchison