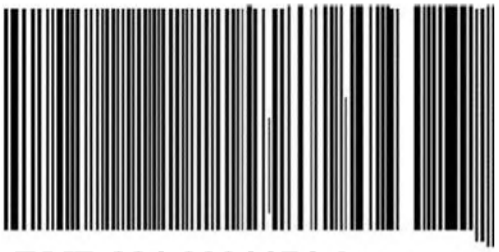
Prepared for OPEN publication in relation to the Independent Inquiry Relating to Afghanistan



RMP-221-0001154-A

Extract - D4123

From: NORTHMOOR TEAM-T1-SIO (Wright, Jason Capt)
Sent: 21 November 2016 09:44
To: NORTHMOOR TEAM-HQ-GoldComd (Harvey, John Maj)
Cc: NORTHMOOR TEAM-HQ-OC (Stitson, Tina Maj); NORTHMOOR TEAM-T1-DSIO2 (Dempster, Mark WO2)
Subject: 20161121-UKSF_Data_Requirement_SO1NM_SIO-OS

Colonel,

I am sure Jim will have articulated why we need all of the ITS1 data from a technical point of view: provenance, forensic integrity and assurance we have all of the data. From me, I would recommend that the language is bland and therefore all I would say is as follows:

The recovery of the redundant ITS1 server is necessary to prove or disprove the most serious of allegations under the remit of Op NORTHMOOR. Likely sources of evidence will be operational planning, its effects, post incident reporting and consequence management. This will likely comprise MS Word documents, various digital media (imagery) and correspondence (email through to formal staff documents).

Background: Significant evidence has already been identified through very limited and constrained searches within UKSF utilising software which is not forensically sound. An earlier method of searching for relevant ESI was considered, using HQ DSF staff. This was discounted due to independence and impartiality concerns together with a lack of forensic provenance. At every stage, RMP have sought to minimise disruption to UKSF and its business; in law we could have chosen to secure and preserve the ITS1 server from the very outset of the enquiry but due regard was given to HQ DSF and its work with a decision to pend recovery. Various other options have been discussed to date, all of which have either failed to be delivered or were not viable.

We know relevant evidence sits on the ITS1 server; there is likely to be evidence in areas that we don't know about (I imagine Jim will have explained this)? The AFG data is spread across the whole data set and is not easily identifiable. Partial recovery may well miss key evidence; cognisance of CPIA is a must. Op NORTHMOOR will hold the data in a classified facility, review the data on a suitably accredited system, operated by people who hold the correct level of security clearance with robust systems in place in order to provide for the security of the ESI.

Total recovery of the data set is essential to prove or disprove the most serious of matters under the remit of Op NORTHMOOR. Not to do so, will result in undue criticism of the RMP in failing to provide for a prompt and effective investigation together unnecessary focus on UKSF. I am sure HQ DSF would wish to be open and transparent, any perceived suggestion of supressing information or evidence will not look good; if there is no 'smoking gun', let us find no evidence of it. Equally, if there is evidence that supports a referral for charge, we must demonstrate the duty of candour and due diligence.

Hope this helps, I realise this is bland but if you wanted to show our hand further, this will need to be on the relevant classification I would not be comfortable with releasing this level of info to HQ DSF although I am aware some of the staff there are read in on the majority of what we are dealing with. Happy to chat securely.

Kind regards,

Jason

Captain J L Wright | Senior Investigating Officer | Operation NORTHMOOR Special Investigation Branch Regiment, Royal Military Police, RAF St Mawgan, Cornwall, TR8 4HP

Contact Details

[redacted]: NORTHMOOR TEAM-T1-SIO

Please note that my email address will change to SIB RMP-NORTHMOOR-T1-SIO on 25 Nov 16.

-----Original Message-----
From: NORTHMOOR TEAM-HQ-GoldComd (Harvey, John Maj)
Sent: 18 November 2016 16:17
To: NORTHMOOR TEAM-T1-SIO (Wright, Jason Capt)
Subject: RE: 20161118_UKSF_Data_Requirement-SO1NM-O

Jason,
Connect with my last; My first draft looks something like this:

As you will be aware Op NORTHMOOR is an independent RMP led investigation into allegations ranging from physical abuse and ill treatment up to murder and or unlawful killing in Afghanistan during the period 2005 to 2013. The allegations were made either directly to RMP by the individual or the Army chain of command, including the UK Detention Oversight Team in Afghanistan or via solicitors acting on behalf of alleged victims.

A main line of enquiry for Op NORTHMOOR is the formal recovery of relevant original electronically stored information (ESI) from a number of MOD data repositories, archives and live servers. This is to ensure that relevant ESI is secured and preserved for evidential production at any subsequent judicial proceedings.

The [redacted] server contains relevant ESI in its original state, which is required for evidential purposes.

Once recovered, the data will be ingested into [redacted] IT system, operated with suitably cleared staff working in a bespoke [redacted] environment.

I understand, as a result of a meeting between our respective staff on Tue 16 Nov 16, that the migration of data from the soon to be redundant server will be complete by 8 Dec 16 and deleting of data from this server will follow.

Your staff ([redacted]) explained that RMP will not be given access to the redundant server without your specific permission.

Hence I am seeking your agreement and assistance in order for RMP to recover relevant data from the [redacted] server.

Until such time as this matter is resolved, I would ask that the data held on the [redacted] server is not deleted or altered in any way.

Regards
Lt Col John Harvey

Op NORTHMOOR | Special Investigation Branch Regiment, Royal Military Police, Bldg 33 , Ward Bks, Bulford Camp, Wiltshire, SP4 9NA.

[redacted]

[redacted]

-----Original Message-----
From: NORTHMOOR TEAM-HQ-GoldComd (Harvey, John Maj)

Sent: 18 November 2016 15:46
To: NORTHMOOR TEAM-T1-SIO (Wright, Jason Capt)
Subject: 20161118_[redacted]_Data_Requirement-SO1NM-O

Jason,
WO2 P, has given me some of the technical!. From your perspective I need the why we need it and what we are after. This will go into a demi official letter from PM(A) to DSF, so needless to say the content will have to be considered carefully.

As previously discussed this is the start of the formal recovery process and I am conscious that time is running out. I would ask that your input is sent to me ASAP.

Happy to chat.

Regards
Lt Col John Harvey

Op NORTHMOOR | Special Investigation Branch Regiment, Royal Military Police, Bldg 33 , Ward Bks, Bulford Camp, Wiltshire, SP4 9NA.

Contact Details [redacted]

[redacted]

-----Original Message-----
From: NORTHMOOR TEAM-Cyber Lead-Priddin JR WO2
Sent: 18 November 2016 14:04
To: NORTHMOOR TEAM-HQ-GoldComd (Harvey, John Maj)
Subject: Forensic Recovery

As discussed

Is this what you needed?

Forensic Recovery

The onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of law enforcement.

Operating systems and other programs frequently alter, add and delete the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed.

Therefore the original data must be preserved, to prove authenticity and integrity of the data and enabling an independent third party to re-examine it and achieve the same result. The preservation process used is called forensic imaging.

Complete or selective forensic imaging are considerations. Complete imaging is self explanatory, the complete recovery of the whole data set. Selective imaging is only considered when it may not be practical or possible to conduct complete imaging. (Point to note : Selective imaging that is too definitive may not be achievable due to technical complications in the storage of the data.)

Selective imaging is a secondary consideration but carries risks as follows:.

1. Lost Evidence. Some data types cannot be recovered through selective imaging such as deleted data or operating system backups. Evidence has already been recovered from these areas from the complete image of [redacted] SFHQ(A) data.
2. Limited Effective Search Capability. Only the data recovered can be searched effectively. Selective imaging limits the search to known storage areas. DSF have already confirmed that the users of the system do not save the data in the relevant known areas and this has been demonstrated to the NORTHMOOR forensic lead.
3. Best Evidence. The police should always recover the best evidence. Complete imaging provides more provenance, authenticity and integrity of the data.
4. Assurance. Complete imaging provides assurance that data does not exist on the system, as it has been searched effectively.
5. Lost Investigation Scope. Data which is not relevant to an investigation and not selectively imaged may become relevant at a later stage.
6. Backups. The backups of the system are also required as they provide a snapshot in time of current data holdings. It will not be technically possible to selectively image a backup tape.

The forensic recommendation is complete imaging.

WO2 P