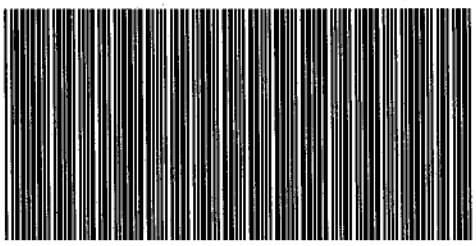
Prepared for OPEN publication in relation to the Independent Inquiry Relating to Afghanistan



RMP-221-00010006-A

[redacted] (SPO CIDU-DCU-CaseMgr8)

From: NORTHMOOR TEAM-Cyber Lead-Priddin JR WO2 <northmoorteam-cyberlead-[redacted]>
Sent: 25 July 2016 10:19
To: NORTHMOOR TEAM-HQ-OC (Stitson, Tina Maj)
Cc: NORTHMOOR TEAM-T1-SIO (Wright, Jason Capt)
Subject: RE: Update

Follow Up Flag: Follow up
Flag Status: Flagged

Ma'am

18-22 Jul 16

Mon 18 Jul 16
Cpl Keen was used for a few hours to forensically copy DVD's recovered from AIr Historic Branch.

Again to maintain a proportionate approach to the data collection the resource at 3C will be used on a Adhoc basis probably for a protracted period. The Data identification in all 3 areas, PJHQ, ATLAS and SF is moving forward. I have made contact with ATLAS now and hopefully have a timeline this week, I just need to discuss a disclosure POC issue with you and then we can move forward. I am still awaiting the first part of the data from SF to be identified, but [redacted] has stated it would be with me last week. I am chasing her. Finally have you had a look at the PJHQ opportunity?

There are still limitations at 3C because of the [redacted] situation,, is there any movement for emergency [redacted]? And have you considered the Bde engagement to make this a higher priority for PJHQ, SF and ATLAS?

We still need to meet so I can brief you on :

1. The Forensic Process - I need to ensure you fully understand the forensic process.
2. Visit Collingwood - Practical understanding of what we are doing and why it's important.
3. Cyber tasking - Covering what we have on now, prioritisation and direction on where we are going.

I am on leave next week for two weeks, but Cpl Mills will be fully briefed and I will still be able to access my email. SSgt Sivieri is also read on the detail also.

WO2 P

From: NORTHMOOR TEAM-Cyber Lead-Priddin JR WO2
Sent: 19 July 2016 14:01
To: NORTHMOOR_TEAM-HQ-OC
Cc: NORTHMOOR_TEAM-T1-SIO
Subject: Update

Ma'am

I will provide a weekly breakdown of what resource we have used from 3C, so you can account for exact demands we have placed upon SPCB 3C on a weekly basis.

Week 11-15 Jul 16

[redacted] * appropriate clearance

Monday 11 Jul 16
WO2 Priddin, SSgt Sivieri and Sgt Ramsden visited DSF in London for a meeting to discuss access and recovery workflow into their data. Sgt Sivieri asked to attend as he is Sgt Ramsden's line manager and he will be managing him during the recovery of data.

Cpl Mills visited PJHQ to discuss access and recovery workflow from their data.

Friday 15 Jul 16
Cpl Keen assisted WO2 Priddin in the preparation of [secure] laptops at 3C for the ingestion of Air Historic Branch data next week.

Summary

The 3C resource used has been adhoc and minimal. The data that is relevant for Team 1 activity is complex and varied. To sustain a proportionate approach to its recovery will take some time to resolve as we are waiting for other organisations to facilitate access and identify these specific pools of data for us. This may need some pressure being applied from above to speed up and I suggest the directorate are engaged to assist. In essence we are not their priority, so someone needs to make us their priority.

There is a serious lack of capability at 3C because of the lack of [*] personnel. All the recovery areas identified require a [**] and most also require [**] Emergency [***] should be considered ASAP, but this may not fix the issue as you cannot be read on to [**] with an emergency [***].

The SPCB MARS system is currently siting outside of its accreditation and [Name Given] does not want to use it until Army HQ have been consulted. This will occur on Thursday.

PJHQ visit has identified a significant opportunity for Op NORTHMOOR. This sits outside of Team 1 activity. [The vast quantity of data held is] relevant to NORTHMOOR investigations require ingestion on to FDHC. This has been planned for post implementation of FDHC at St Mawgan. This process is significant and will take some time to forensically ingest and will become NORTHMOOR main delay after FDHC has been implemented, as you will obviously want to search that data ASAP to move investigations forward. Stage 3 of the Holmes implementation tries to reduce that delay post implementation of FDHC, to start forensic ingestion before hand, but that has not even been scoped. PJHQ have offered to work with NORTHMOOR, which I believe could assist the process greatly. This will involve procurement of hardware that was not planned, but so would stage 3 of Holmes. We would also require a Forensic Analyst to lead the process on a day to day basis and additional manpower from NORTHMOOR. There will be a training implication but that was foreseen and just needs to brought forward.

Finally I wanted to highlight areas of delay for you. The [SFHQ (A)] data from Afghanistan could only be processed on a [higher classification] system. The implementation of that system delayed the access to that data. The [ITS1] system was assessed late last year and Op NORTHMOOR have not had the resources to start the work on it till now. The PJHQ data is not Team 1 activity and was not started due to lack of resource and appropriately [cleared] personnel.

I recommend we meet this week and go through 3 areas:

1. The Forensic Process - I need to ensure you fully understand the forensic process.
2. Visit Collingwood - Practical understanding of what we are doing and why it's important.
3. Cyber tasking - Covering what we have on now, prioritisation and direction on where we are going, out.

WO2 P

[* appropriately cleared]
[** higher classification]
[*** appropriate clearance]