NORTHMOOR TEAM-T1-DSIO2 (Dempster, Mark WO2)

From: NORTHMOOR TEAM-T1-SIO (Wright, Jason Capt)
Sent: 07 October 2016 14:25
To: Army PM-AH-TECH (Morris, Rob Col)
Cc: NORTHMOOR TEAM-HQ-GoldComd (Harvey, John Maj); NORTHMOOR TEAM-HQ-OC (Stitson, Tina Maj); NORTHMOOR TEAM-T1-DSIO2 (Dempster, Mark WO2); NORTHMOOR TEAM-Cyber Lead-Priddin JR WO2
Subject: 20161007-IRTB_ITS1_SIO-OS

Colonel,

Issue: Requirement to recover the redundant ITS1 server.

Recommendations: AH Tech is requested to:

- Secure agreement with data owner for RMP to recover in total the redundant ITS1 server (circa 16 Nov 16);
- Provide assurance to the data owner that the information and material will be recovered, treated and stored in a manner commensurate with its security classification.

Timing: Routine, noting that data migration commenced on 3 Oct 16 and scheduled to complete on 16 Nov 16.

Background: A main line of enquiry for NORTHMOOR Team is the formal recovery of 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 exploitation and production at any subsequent judicial proceedings. The ITS1 server contains relevant ESI in its original state, required for evidential purposes in pursuit of the most serious matters; this cannot be achieved in a piecemeal manner; the whole server in its original format must be recovered, to do otherwise risks loss of evidence. Once recovered, the data will be ingested into a system of a certain classification, operated with suitably cleared staff working in a bespoke classified environment.

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

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

NORTHMOOR Team/Team1/Correspondence

6 Oct 16

Gold Comd

Copy to:

OC NORTHMOOR Team
MIR

FORENSIC RECOVERY OF THE [redacted] SERVER

1. On Tue 25 Mar 14, direction was received from HQ PM (A) to investigate the circumstances of numerous complaints brought by Afghan nationals who alleged that between 2005 and 2013, they had been subjected to varying degrees of criminal and non-criminal behaviour by UK Armed Forces personnel in Afghanistan.

2. A number of the complaints involve operations conducted by specific UK force elements.

3. A main line of enquiry for NORTHMOOR Team is the formal recovery of electronically stored information (ESI), from a number of MOD data repositories, archives and live servers. The [redacted] system is a centralised data server located within a UK garrison; it stores a large amount of relevant ESI protectively marked as [redacted], likely to form essential evidence in NORTHMOOR enquiries. The formal forensic recovery of [redacted] by RMP will facilitate investigative exploitation of this data set and ensure that relevant ESI is secured and preserved for any subsequent judicial proceedings in accordance with national guidance and best practice in such matters.

4. In order to preserve the provenance and integrity of the data set and to minimise the risk of ESI being altered or destroyed, [redacted] will be secured and forensically recovered as soon as practicable. This cannot be done in a compartmentalised manner as relevant data is stored across the whole system and whilst it is recognised that in recovering the server, non-relevant ESI will be in the possession of RMP, assurance of data security can be provided; once recovered, the data will be ingested into a [redacted], operated with suitably cleared staff working in a bespoke [redacted] enviornment. Specialist cyber support from suitably qualified and experienced personnel will be required from SPCB 3C, in support of the NORTHMOOR Cyber lead, WO2 Priddin J, RMP (SIB).

5. The [redacted] system is currently undergoing a technical replacement process, resulting in the server currently in use being made redundant and therefore available for immediate forensic recovery by the NORTHMOOR Team. It is anticipated that the upgrading process will be complete on or around the 16 Nov 16. Recovery of the redundant server will obviate any operational impact to the data owner and progress the promptness and effectiveness of the invesitigation.

Signature: *C A Pritchard*
Pritchard C A
Sgt

Authenticated: *J L Wright*
J L Wright
Capt
SIO

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

[redacted] SERVER 06 Oct 16

Capt Wright Submitted a LM to Lt Col Harvey, Gold Comd.