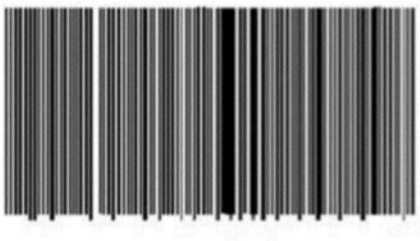
Prepared for OPEN publication in relation to the Independent Inquiry Relating to Afghanistan



RMP-221-0007045-A

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

SPCB/03/03/02

8 Jan 16

SO1 IS G6 – Army HQ

Copy to: SO2 G1 G4 G6-HQ PM(A) & HQ 1 MP Bde CO Spec Ops Regt RMP

BUSINESS CASE FOR BESPOKE FORENSIC RECOVERY AND EXPLOITATION SOLUTION – Op NORTHMOOR.

References:

A. Armed Forces Act 2006

B. ArmySec/03/08 MS411 – MinSub to SofS - Op NORTHMOOR Investigations Into Detainee Abuse Allegations In Afghanistan

INTRODUCTION

1. **There is a requirement for the provision of an independent, stand alone scientific system used to process and review forensic electronic/digital evidence as part of an enduring Major Incident Unit (MIU) for the Service Police (SP) to be able to meet its statutory obligations (Ref A) to undertake European Convention of Human Rights (ECHR) compliant** [of a certain classification] **complex investigations comprising of a Major Incident Room (MIR), digital forensic capability and a review suite for use by the RMP[1] within the UK**. This requirement is not only required for the legislative reasons at Ref A but also because there is no digital forensic recovery solution within the UK or Europe which could complete the task required. This will involve the exploitation of many different types of digital media including hard disk drives, CD, DVD, CD ROM, USB, paper documents requiring scanning, which will be forensically[2] ingested into the system and reviewed for investigative relevance and then produced in an evidential format. This is a large scale operation initially encompassing approximately [NG] digital storage devices and a yet to be determined number of paper exhibits. This capability will provide RMP and potentially the wider SP with an enduring digital forensic capability to investgate complex criminal investigations or other major incidents involving the military, whether operationally related or during peace time activities. This is necessary to support and progress a large number of current criminal investigations and to support the MOD in the current legal challenge of Public Inquiries (PIs), Judicial Reviews (JRs) and Personal Injury claims. The requirement is for the RMP to be equipped with a bespoke independent, stand alone scientific forensic system to:

a. Ensure the forensic evidential integrity of all relevant data from the point of collection through to dissemination and archive using digital forensic tools (software and hardware) that meet ACPO[3] standards relating to the processing of all forms of electronic data;

b. Enable the forensic import of all forms of data (including deleted, fragmented, corrupted, and encrypted files together with any associated metadata) onto a high speed forensic data storage facility;

[1] RMP for Op NORTHMOOR

[2] [details of digitial interfaces].

[3] ACPO is now known as the National Police Chiefs Council

c. Enable forensic storage (incl backup) using 12 PB of storage with 6 PB of usable storage data up to and including [redacted: a certain classification];

d. Enable a team of 85 forensic analysts and investigators (with surge capacity up to 120 personnel) to:

(1) Conduct simultaneous detailed complex keyword searches across an entire data set.

(2) Identify duplicate documents.

(3) Preview documents and mark them as to their relevance for later review by a Senior Investigating Officer (SIO).

(4) Produce electronic evidence from the forensically recovered data in accordance with ACPO guidelines[4].

e. Enable the disclosure of relevant material to a standard that meets the provisions of both the Criminal Procedure & Investigations Act 1996 (CPIA96) and Part 31 of the Civil Procedure Rules for England & Wales[5] (Practice Direction 31B – Disclosure of Electronic Documents) (CPR).

BACKGROUND

2. The Armed Forces Act 2006 requires all allegations of criminal activity by Service Personnel to be investigated by the Service Police. Where allegations relate to unlawful killing or the infliction of cruel, inhuman or degrading treatment, investigations must comply with the European Convention on Human Rights (ECHR).

3. Op NORTHMOOR as briefed to the Secretary of State, (Ref B) is the ongoing investigation by SIB Regt RMP into allegations of mistreatment of 141 Afghan detainees whilst in UK custody between 2005 and 2013. To meet the standards expected by the Courts, the investigation requires a dedicated facility and specialist IT to store and examine significant amounts of electronic data and protectively marked material including [redacted: a certain classification.] Lee Day & Co Solicitors (LDC) have sent the MOD pre-action protocol letters relating to 80 of the Afghan complainants. These civil claims against the MOD have been stayed by the High Court until October 15 when they will be reviewed again. In order to stay the claims further, the Courts require that the MOD demonstrate progress in the investigation including the establishment and acquisition of the necessary facilities and equipment to carry it out.

4. The investigation is likely to last in excess of 2 years and possibly out to 5. For routine purposes there will be 85 forensic analysts and investigators supported by a small cadre of 10 military support staff and 4 x Civ Staff. There may be the requirement to surge the forensic analysts and investigators up to 120 pers should the investigative workload dictate this. The civilian and military support staff will not require access to the forensic and recovery system[6]. The current adhoc facility utilised by Op NORTHMOOR personnel is located with the SIB Regt in Campion Lines, Bulford. This facility is not [redacted: suitably cleared] and therefore is not suitable.

---

[4] ACPO evidential and investigative principles are published in the ACPO (and National High-Tech Crime Unit) *'Good Practice Guide for Computer-Based Electronic Evidence'*.

[5] *Vide* Civil Proceedings Rules (CPR) Practice Direction 31B – Disclosure of Electronic Documents.

[6] A separate SON has been submitted for DII[redacted] and DII[redacted] requirements. DII[redacted] and DII[redacted] will be used for JPA, e-mail and other communication needs but not as a communication medium for any [redacted: data of a certain classification.]

5. The Campion Lines facilities extend to a single two story building providing office space for RHQ SIB Regt, HQ 4 Inv Coy, an Ops Pl, 32 SIB Sect and PS & R, as well as the current adhoc Op NORTHMOOR facility. The building is due to undergo significant upgrading in early 2016 which is likely to involve SIB Regt vacating the site for 6-9 months. Other than car parking Campion Lines has no other facilities on site.

6. In addition, a site survey by [redacted: security officer] has shown that even following the upgrade, Campion Lines will never be a suitable location for the classification and quantity of material being held for the current investigation or the additional technical equipment which needs to be installed to facilitate data analysis. As a result DIO are sourcing a suitable location which meets the requirements.

REQUIREMENT

7. There is a requirement for a stand alone, scientific system used to process and review forensic electronic/digital evidence in accordance with UK ACPO guidelines. This is required to support Op NORTHMOOR as briefed to the Secretary of State, (Ref B) which is the ongoing investigation by SIB Regt RMP into allegations of mistreatment of 141 Afghan detainees whilst in UK custody between 2005 and 2013. To meet the standards expected by the Courts, the investigation requires a dedicated facility and specialist IT to store and examine significant amounts of electronic data and protectively marked material including [redacted: a certain classification]. There is no facility within the UK or Europe which could be used for an investigation of this size, complexity or [redacted]; therefore this is a unique requirement. It must be accredited [redacted: above a certain classification] and the proposal is for a dedicated [redacted: computer forensic LAN] [redacted: of the required classification] to be based at RAF St Mawgan (TBC) not to exceed a total cost of £7.5m (VAT excluded) for initial procurement. Initially the framework and 12PB of storage with built in replication and RAID will be purchased. The requirement must be capable of hosting HOLMES[7] and I2[8] intelligence suite. The requirement for this storage is based on the calculations using Moore's Law based on the amount of data and hardware initially preserved, experience from previous large scale investigations (IHAT)[9].

8. The dedicated standalone LAN must be capable of hosting industry standard computer forensic tools which is the only method by which an investigation team can quickly, and to standards set by ACPO concerning electronic computer investigations, recover, search, utilise and disclose vast volumes of electronic data.

Hardware Requirement

9. The Information System (IS) needs to be based on a proven reference architecture that supports many of the core forensic software packages such as [redacted: list of software packages] [redacted], etc. The proposed solution must allow for real-time analyst collaboration on individual or multiple cases, possibly scaling up to 120 users. The estimated storage requirement is 6 PB of useable storage with built in replication and RAID.

Server Based Processing.

10. The IS solution must maximise productivity/efficiencies by utilising a high performance computer cluster (HPCC) for the processing of digital evidence whilst simultaneously allowing the investigation teams to view processed evidence without impacting the performance.

---

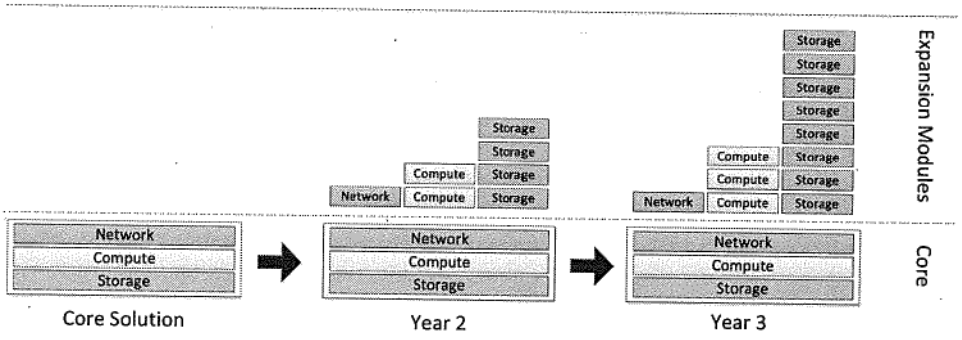
[7] HOLMES is the Home Office Large Major Enquiry System which is an investigative management tool capable of handling thousands of lines of enquiry and cross referencing evidence.

[8] I2 is a suite of applications used for the management and exploitation of intelligence.

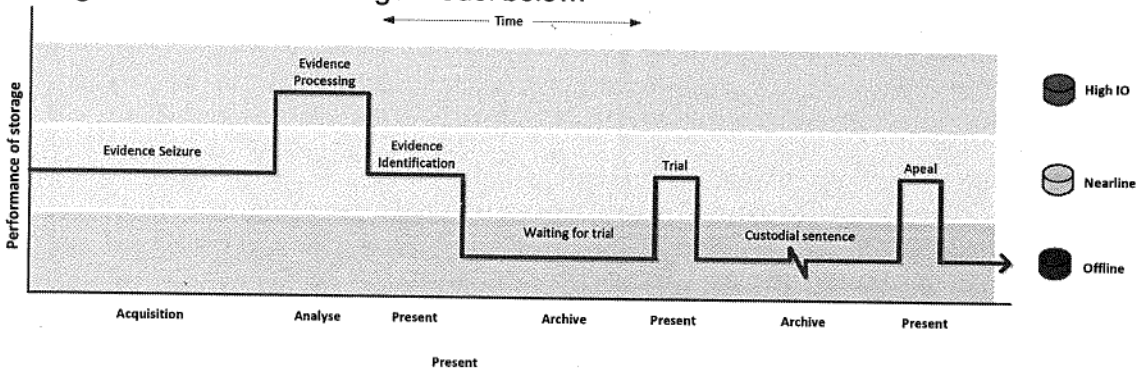
[9] This is 6PB.

a. It must have high speed core network backbone for decreasing image ingestion[10] and data movement times. Due to the ever increasing images sizes in digital forensics the need for a fast, low latency interconnect between virtual machine servers, file servers and analyst/ingestion clients is critical. The solution must support a high speed core network to facilitate the fast transfer of multiple terabyte images between devices.

b. The IS solution must create a common processing and storage solution from which to build a leading edge forensic capability. The IS solution must be designed to scale without the requirement to replace core components. The hardware needs to be capable of processing large amounts of data in short time frames. The storage needs to be capable of supporting the processing capability. The desire is for the solution to be expandable by simply adding more hardware and software modules (As per diagram below).



11. An intelligent storage solution is required to provide centralised data storage for the unit. It must be a tiered solution that provides fast response to frequently accessed cases and be able to automatically migrate old cases or files to an archived area to balance disk performance. Future expansion of the storage without the need for expensive controllers and a mix of different speed disk drives is essential. It is anticipated that the case life cycle management will fit the storage model below:



Client Access

12. Due to the security classification of the data it is the preferred solution to use 100 diskless workstations with dual monitor capability for the investigation teams to access the

[10] An estimated requirement of high spec UADs x 40 for data ingestion based 500Gb drive taking 24hrs to image each terminal capable of imaging 3 devices simultaneously real estate limitations.

data. Due to unknowns around future tools and types of data we would request the ability for a flexible workstation that can be either a zero client (initial solution) or run a full operating system with the proviso that once powered off has no data remaining on the system (diskless in full OS and zero client mode). All investigative work will be completed on this system.

13. It is a requirement that all desk top access points have dual factor authentication, smart card and PIN and user password.

Software Requirement

Forensic Software

14. The forensic software must be capable of:

a. **Evidential Integrity.** The software will need to provide a method for proving the evidential Integrity of the digital evidence once ingested/copied onto the system. This data will also need to maintain its evidential integrity even if copied externally.

b. The software must be capable of processing large quanities of data in limited timescales using all of the resources of the hardware provided. The LAN fibre speeds will need a minimum standard providing minimum latency and high bandwidth[11].

c. The software must provide the user with the capability of reviewing large quantities of data using intelligence search methods such as index key word searching, identification of data category types and manual review at the binary level.

d. The software must provide a report function in the form of digital evidence in accordance with ACPO guidelines.

e. The software must provide a full audit trail of actions taken by users.

Virtualisation Software

15. The IS solution must utilise virtual technologies (which can support 85 users with a surge up to 120 users) to allow the move away from traditional client based activities. Virtual technologies are also essential to reduce the amount of hardware required to run the units specialist software from virtual servers and allow processing of multiple cases for each analyst.

Dual Factor Authentication Software

16. The IS solution requires dual factor authentication at the end point.

Backup Solution

17. The IS capability requires a tiered back up solution which would include a magnetic tape capability and data replication for business critical data and disaster recovery off floor plate. The business critical evidence and data will be replicated within two areas of the IS solution. This is to safeguard against disc failure and provide evidential resilience.

System Support

[11] 10Gbps network speed required.

18. The warranty includes a 4 hour response with no additional cost. However no components (even if faulty) and very little diagnostic data may be taken offsite. All engineering resource attending site must be cleared. The system will have no remote support capability.

Training Requirement

19. Should the final software solution for the IS requirement not be part of the current forensic capability then a training cost, time frame to deliver and impact to investigative delay will be required for practitioners.

System Design

20. The IS solution must be built on a Microsoft Windows network using the latest version of Microsoft Windows Server and support up to 85 users with the potential to expand to 120 users. The solution needs to be scalable and have redundancy built in to provide business as usual in the event of a hardware or software failure. Microsoft OS as it is the only platform capable of supporting the operation of all known industry standard forensic software suitable for this requirement.

21. The IS solution should be built as an enduring project with the ability to expand or upgrade if required. Since the formation of Op NORTHMOOR, the allegations and scope of the investigation have increased dramatically and there is an expectation this course of action will continue. The proposed network diagram is at Annex A.

22. Op NORTHMOOR personnel will require the relevant training on the IS solution and associated supporting systems once they are operational to ensure all users can conduct the appropriate and mandatory functions in support of their duty. This will assist the investigation to withstand any legal challenges that may be forthcoming in any future proceedings that may arise.

Installation

23. The system **must** be built using suitably cleared workers who will be escorted. A single supplier solution is required so that both software and hardware are installed with minimal risk to failure. Hardware and software could be supplied seperately but adds risk. Due to this risk, it makes sense that the provider also provides a single supplier solution for the maintenance contract.

24. **ACPO National Standards concerning Electronic Data**. For criminal investigations, ACPO has provided the following guidelines concerning the forensic processing of digital evidence. These guidelines are self explanatory, and on which the principles of computer/digital forensics are based and considered to be acceptable in UK Courts:

a. **Principle 1** - no action taken by Police or their agents should change data held on a computer or other media, which may subsequently be relied upon in Court;

b. **Principle 2** - in exceptional circumstances where a person finds it necessary to access original data held on a target computer, that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions;

c. **Principle 3** - an audit trail or other record of all processes applied to computer based evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result; and

d. **Principle 4** - the Officer in charge of the case is responsible for ensuring that the law and these principles are adhered to. This applies to the possession of and access to, information contained in a computer. They must be satisfied that anyone accessing the computer, or any use of a copying device, complies with these laws and principles.

25. **Civil Procedure Rules (CPR).** In civil proceedings (JR and PI claims) data recovered from differing mediums without using recognised industry standard forensic tools will not conform to the provisions of CPR, which defines an electronic document as:

> *"any document held in electronic form. It includes, for example, e-mail and other electronic communications such as text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones. In addition to documents that are readily accessible from computer systems and other electronic devices and media, it includes documents that are stored on servers and back-up systems and documents that have been deleted. It also includes Metadata and other embedded data which is not typically visible on screen or a print out."*

In addition, the High Court has directed[12] that backup disks and systems be searched for data that had been deleted from primary data servers. Therefore it is vital the RMP uses an industry standard tool for the forensic recovery, analysis and disclosure of all file types including deleted, password protected, encrypted and fragmented documents from all data sources. This can only be achieved with a high speed forensic LAN.

OPTIONS CONSIDERED

26. **Option 1 – Do Nothing**. This option will not be considered further as it will:

a. Fail to meet the requirements of the court, to conduct the forensic search of data to appropriate standards;

b. Prevent the RMP from undertaking an effective investigation as required by AFA 06 and the ECHR;

c. Attract further political and public criticism of the SJS; and;

d. Attract significant additional costs relating to JR and PI claims.

27. **Option 2 – Use IHAT**. This option was considered but as IHAT is not cleared to [redacted] classification this option is discounted.

28. **Option 3 – Utilisation of the DJEP Archive System (DAS)**. This is a system, which currently contains data recovered from hard-drives emanating from relevant areas:

a. **Advantages.**

(1) No cost to Army TLB/RMP.

b **Disadvantages.**

(1) It is situated within PJHQ and controlled by non-RMP personnel therefore

[12] *Vide* Digicel (St Lucia) v Cable & Wireless [2008] EWHC 2552 (Ch).

any searches conducted on this system do not conform with the ACPO principles and may be deemed to not have been conducted independently;

(2) It does not have any capacity for the forensic ingestion of data and does not have any capacity for the forensic recovery and processing of deleted, fragmented, hidden, encrypted, password protected files;

(3) Any searches cannot be guaranteed to be thorough as deleted, hidden, meta-data, encrypted, and corrupted files cannot be identified and examined for relevance;

(4) It does not conform the ACPO Guidelines and therefore any information produced directly from this system is unlikely to be admissible in Court; and

(5) It only holds [redacted] protective marking.

29. **Option 4 – Procurement of a Standalone Dedicated Computer Forensic LAN.** The Service Police Crime Bureau (SPCB) has significant experience having successfully implemented a number of similar systems for high level and complex investigations. This cumulative knowledge, experience and recent market research in this technical area of expertise has led to this preferred option. The options for suitable locations have been explored with DIO to ensure timeliness, cost and VfM are attained.

a. **Advantages.**

(1) Enables RMP to maintain independence in the recovery, search and processing of relevant data in support of investigations.

(2) The identified system will enable multiple users to access digital evidence for review and identification of lines of enquiry whilst maintaining forensic integrity and auditability.

(3) The system identified can be delivered and be operational within 6 months of purchase and has sufficient scalability to add additional tools and storage to potentially provide a future SP and [redacted] investigative environment.

(4) The forensic tools are fully able to forensically recover all file types (including corrupted, fragmented, deleted and encrypted files) to a standard that is acceptable to all UK Courts.

(5) Locating the system with RMP will enable them to have dedicated and immediate access to all recovered data.

(6) The proposal covers the entire life span of the data from collection and ingestion through to disclosure: all to ACPO and the CPR Practice Direction 31B standards.

b. **Disadvantages.** It is assessed that the only disadvantage with this option is the cost of hardware at approx £6.5m (exclusive of VAT) and software at approx £1m (exclusive of VAT). However, this is mitigated against the significantly higher tangible cost of reputational damage through lack of high level investigative capability and potential expense through civil litigation.

30. **Recommended Option**. **Option 4** – procurement of a dedicated computer forensic LAN is the recommended option at a cost of approx £7.5m (exclusive of VAT) for the reasons identified at paragraph 27a.

31. **Procurement Strategy**. Procurement should be undertaken through IS procurement and CCS. The initial purchase will encompass the framework and 12PB solution. Due to the unknown amount of data required for Op NORTHMOOR capability for further expansion is required.

32. The IS solution provider must provide a law enforcement (UK) reference at a certain classification or above. This is to remove the possibility of failure knowing that the provider has successfully conducted work of a similar nature.

33. The IS solution provider must be able to demonstrate that they have implemented working solutions of this nature and scale with recognised forensic software providers. The software should be the most up to date available to fit with the investigation requirement and compatible to the hardware. The software provider must ably demonstrate they have implemented working solutions of this nature and scale with a hardware provider. This is to minimise the risk of failure at implementation and subsequent delay.

34. The IS solution provider must provide the IS solution within costs. The provider should build the system as an integrated system (software and hardware) as a single supplier. The maintenance contract must be similarly run as a single source supplier by the provider.

35. **Through Life Costs**. The through life costs are:

a. **Hardware**. The initial hardware framework cost is **£4.5m**. The first uplift is **£1m** with a potential further uplift at **£1m**. These costings are exclusive of VAT. The further uplifts may be required during a single financial year if the usable storage is consumed. Any delay in acquiring additional storage would impact on the investigation and cause unnecessary delay. The hardware must come with an inclusive five year hardware maintenance contract.

b. **Software.** The initial cost of approx **£1m** for forensic software, licensing and warranty from the provider for five years.

36. **Costing Options**. The two options below show how costs can be spread through life. The preferred option is Option 1 as it would allow the cost to be spread over three financial years. The initial cost in FY15/16 will be £5.58m for hardware and software.

Option 1

37. This is a modular option which spreads the cost over 2 financial years. This would allow for storage requirements to be accurately assessed and purchased as required. However, delay in purchasing could impact and further delay the investigation. All costs below are exclusive of VAT. For FY 2020 – 2025 the ongoing hardware and software costs have been added to ABC16. **Option 1 is our preferred option.**

Option	FY15/16	FY16/17	FY17/18	FY 18/19	FY 19/20	FY 20/21 -24/25
1	Hardware Framework **£4.5** Software, licensing, **£1m** **£80k** CIS reqts **Total £5.58m**	£2m Hardware uplift		No Cost	No Cost	Hardware £1m Software £250k

Option 2

38. This option would see the purchase of the entire solution within FY 15/16. There is no way to accurately estimate the ingestion time for the forensic data. It is an aspiration to have completed this process within 12 months so avoiding delay. £7.58m has been set aside for this expenditure within this financial year. Costs below are exclusive of VAT. For FY 2020 – 2025 the ongoing hardware and software costs have been added to ABC16.

Option	FY15/16	FY16/17	FY17/18	FY 18/19	FY 19/20	FY 20/21 -24/25
2	Hardware Framework £6.5m Software, licensing, support £1m £80k CIS reqts	No cost	No cost	No Cost	No Cost	Hardware £1m Software £250k

39. The Cabinet Office have advised the stakeholders in this business case to push forward with competitive tender. It is anticipated that this will clarify costing requirement which may lead to savings.

40. **Stakeholders**.

a. PM(A) on behalf of RMP.

b. DJEP in assisting the SoS's defence in civil proceedings.

c. Associated [redacted] and SF

d. Associated [redacted] and SF [redacted security officers].

41. **Governance**. Governance of the computer forensic LAN will rest with PM(A). The solution delivery will be evaluated by OC SPCB with any issues raised to Army HQ G6.

42. **Timelines**. Installation should take approx 12 weeks following accreditation with DAIS and any security works services that may be required. It should be noted that prior to commissioning, HQ PM(A) will be required to produce detailed RMADs in order to enable appropriate security accreditation of the system before any data is ingested onto the LAN.

SUMMARY

43. The importance of this project cannot be overstated. The ability of the RMP to undertake investigations effectively, independently and to relevant national and international standards is fundamental to the credibility and competence of the SJS. Given the historical nature of all the allegations, it is absolutely essential for the MOD to have a dedicated capability to forensically recover and search a significant volume of data in order to prove or disprove each allegation. This can only be achieved through the use of a dedicated computer forensic LAN which can hold a significant quantity of [redacted required] data.

PAL Hacker
Maj
For PM(A)