

30 April 2008



Final Report

Report into the Loss of MOD Personal Data

For Permanent Under Secretary Ministry of Defence

Sir Edmund Burton

BURTON REVIEW – CONTENTS

1. Preface
2. Preliminaries - Review of MOD Protection of Personal Data
3. Part One - The Main Circumstances and Events That Led to the Loss by MOD of Personal Data on 9 January 2008
4. Part Two - MOD Protection and Management of Personal Data

Annexes:

- A. Summary of Recommendations
- B. List of MOD Interviewees
- C. Glossary of Terminology
- D. Abbreviations and Acronyms
- E. Data Protection Act 1998 (extract)
- F. Chronology of TAFMIS Events
- G. TAFMIS Programme Governance (TAFMIS Sy Ops)
- H. TAFMIS Programme Governance (AG Perspective)
- I. DataVault User Instruction (extract)
- J. Defence Information Infrastructure (DII)
- K. MOD Departmental Structure for Implementation and Compliance with DPA 1998
- L. The Organisation of the MOD's Security Stakeholders

PREFACE

NATIONAL INFORMATION ASSURANCE STRATEGY

1. The National Information Assurance Strategy, originally issued in 2003, was revised and re-issued in 2007. The strategy seeks three strategic outcomes:
 - a. Government is better able to deliver public services through the appropriate use of Information and Communications Technology (ICT).
 - b. The UK's national security is strengthened by protecting information and information systems at risk of compromise.
 - c. The UK's economic and social well-being is enhanced as government, businesses and citizens realise the full benefits of ICT.
2. The Strategy asserts that Information and Communications Technologies (ICT) are a critical business asset for any organisation and that their exploitation is fundamental to the achievement of business objectives.
3. Following the publication of the 2003 Information Assurance Strategy, the Cabinet Secretary issued directions that departments were to appoint a Senior Information Risk Officer (SIRO), at board level, who understood the business goals of their organisation, and was to ensure that the management of information risks was weighed alongside the management of other risks facing the organisation, such as financial, legal and operational risks. This direction was re-iterated by the Cabinet Office earlier this year.
4. In June 2007, the revised strategy stated that the strategic outcomes would be achieved by focussing on the following objectives:
 - a. Clear and effective information risk management.
 - b. Clear board level ownership and accountability for information risks.
 - c. Where information is shared, a single point of risk ownership is to be identified.
 - d. Agreement upon and compliance with approved and appropriate Information Assurance standards.
 - e. Development and availability of appropriate Information Assurance capabilities.

BRITISH DEFENCE DOCTRINE

5. At the heart of British Defence Doctrine lies the Manoeuvrist Approach, a key enabler of which is the concept of Information Superiority. This approach is developed in the MOD's thinking on Network Enabled Capability. The exploitation of information and its protection are, therefore, fundamental to the business of the Ministry of Defence, the Armed Forces and their commercial partners.

SHARING INFORMATION

6. One of the themes emerging from the Strategy for Transformational Government (2005) was the increased emphasis on sharing services, particularly in information and infrastructure. The Armed Forces have been early pioneers of this approach, through a range of Private Finance Initiative (PFI) and Public Private Partnership (PPP) contracts. In the operational arena, decades of experience of operations in coalitions and with allies, and in international collaborative programmes, have provided experience of the risks and benefits of sharing sensitive information.

7. The management of risks in a situation in which there is a dependence on a partner calls for particular attention in the governance arrangements, active leadership and clear direction on accountabilities. Despite careful contractual statements, operational and reputational risk will remain with the government customer. Such risks need to be jointly, and carefully, defined and jointly managed. This is not yet widely acknowledged and avoidable risks are unaddressed.

PROFESSIONALISM

8. The Strategy for Transformational Government acknowledged that “the Government’s ambition for technology enabled change is challenging, but achievable, provided it is accompanied by a step-change in the professionalism with which it is delivered. This requires: coherent joined up **leadership and governance; portfolio management** of the technology programmes; development of IT **professionalism and skills**; strengthening of the controls and support to ensure **reliable project delivery**; improvements in **supplier management**; and a systematic focus on **innovation**.”

9. During the Cold War, awareness of real security was ingrained in individuals and organisations. Audit, inspection, and compliance regimes were rigorously underpinned by codes of discipline. These well developed processes and procedures have not been translated, effectively, into the information age. Furthermore, there seems to be a lack of awareness that, in the information age, the behaviour of each individual is a significant factor in the risks faced by the parent organisation. Achieving such awareness and appropriate codes of personal and corporate conduct, with effective governance, represents an urgent, high priority task for leadership teams across the UK: in central and local government, across the private sector, academe and throughout the education community.

REVIEW OF MOD PROTECTION OF PERSONAL DATA

AIM

1. The aim of this work was to review the Ministry of Defence (MOD)'s protection of personal data in the wake of the theft (on 9 January 2008) of a Royal Navy (RN) recruiter's laptop, which contained unencrypted personal records for more than 600,000¹ people.
2. The Review was carried out in line with the Terms of Reference from the Secretary of State for Defence.

“To establish the exact circumstances and events that led to the loss by MOD of personal data; to examine the adequacy of the steps taken to prevent any recurrence, and of MOD policy, practice and management arrangements in respect of the protection of personal data more generally; to make recommendations; and to report to MOD's permanent secretary not later than 30 April 2008”

SCOPE

3. The main body of this report is in two parts. Part One sets out a detailed narrative of the events leading up to the loss of data on 9 January 2008, covering all relevant issues surrounding the Training Administration and Financial Management Information System (TAFMIS) system and the attendant policies and procedures. Part Two considers the broader MOD approach to personal data protection. Both parts contain recommendations, which are summarised at Annex A.

CONTEXT

4. On 21 November 2007, following the data loss from Her Majesty's Revenue and Customs (HMRC), the Prime Minister commissioned a report on “Data Handling Procedures in Government”. An interim report was published in December 2007, with recommendations. Subsequently, the Cabinet Office issued a series of minimum mandatory measures to be adopted by all Government departments. The MOD is implementing these measures.
5. Laptop Loss: 9 January 2008. On 9 January 2008 a TAFMIS laptop, containing approximately 600,000 personal records of recruits or potential recruits, was stolen from an RN recruiter in Birmingham. The timetable of subsequent events can be summarised as follows:
 - a. 11 January. Incident was reported to Ministers.
 - b. 14 January. Ministers were informed that the data were not encrypted.
 - c. 16 January. MOD HQ ordered recall of all TAFMIS recruiter laptops.

¹ This figure refers to the personal records for recruits and potential recruits. There were also an additional c400,000 next of kin and referee records on the database.

d. 21 January.

(1) Secretary of State made a formal statement to the House of Commons announcing that he had invited Sir Edmund Burton to undertake a full investigation, noting that the report would be made available to the Information Commissioner.

(2) MOD appointed a Head of Data Protection and Information Assurance.

(3) Following a directive from the Cabinet Secretary, the MOD instructed Top Level Budget (TLB) Holders and Agency Chief Executives to halt movement of unencrypted laptops and removable media, such as Universal Serial Bus (USB) sticks.

e. 5 February. Burton Review Team Assembled in MOD.

f. 30 April. Burton Review Report handed to Permanent Under Secretary MOD.

EXECUTIVE SUMMARY

TAFMIS

6. In 2001 MOD HQ set in place the governance processes necessary to meet the obligations under the Data Protection Act. Instructions issued in 2001 included the appointment of a cadre of named Data Protection Officers. This list included the Data Protection Officers for the Army Training & Recruiting Agency (ATRA) (now the Army Recruiting & Training Division (ARTD)) and for the individual service recruiting organisations.

7. The stolen laptop, designated TAFMIS-R(H)SQL, was one of a small population of, currently, 51² laptops, which hold a large database incorporating over 600,000 personal records. Investigations revealed that a total of 4 of these laptops have been stolen since 2004 (all from parked cars). Only the recent theft appears to have led to disciplinary proceedings. Although the security instructions for the safe-keeping of laptops were clear in prohibiting them from being left in unattended vehicles, they did not dictate that the data must be encrypted.

8. However, there is no evidence to confirm that the data protection aspects arising from the RN/RAF requirement for a substantial database, available for use on a laptop, had been formally addressed, either by the service sponsors, or by the contractor.

² The total number of TAFMIS R(H) SQL laptops quoted at various points in this report varies. This is because the number in use at any given moment changed as individual laptops were lost, stolen, became unserviceable or were replaced.

9. It is likely that the Department was in breach of several principles set out in the Data Protection Act, as soon as the large TAFMIS recruit database was implemented and then made available on unencrypted laptops. However, the principles are not precise: they require judgment. The Department will, therefore, need to seek guidance on the exercise of that judgement from the Information Commissioner.

10. The evidence indicates that the overall management of the TAFMIS project lacked rigour. Consequently, it has proved impossible to trace records of requirements, approvals, decisions and actions at key stages. Both parties (ARTD and the prime contractor, Electronic Data Systems (EDS)) will wish to take appropriate action.

DEFENCE COMMUNITY ISSUES

11. The Department is not treating information, knowledge and data as key operational and business assets.

12. Information risk is not being formally managed at executive boards across the Department, with a small number of exceptions. This constitutes a significant risk to the Department's operational effectiveness, resilience and reputation.

13. Generally, there is little awareness of the current, real, threat to information, and hence to the Department's ability to deliver and support operational capability. Consequently, there can be little assurance that information is being effectively protected.

14. However, the Department instigated a major review of departmental Information Assurance (the Rowlinson Review) in 2005. The comprehensive programme of work is well underway. The Department's intent to integrate this with the work emerging from the Cabinet Office Review is supported. Success of the overall programme will depend, significantly, on support and leadership across the Department.

15. Outside MOD HQ, with a few notable exceptions, there is very limited understanding of the Department's obligations under the Data Protection Act. However, within the Deputy Chief of the Defence Staff (Health) area, there are firm obligations to protect and manage data in accordance with the Caldicott principles for medical data guardianship. These may well be adaptable to meet the wider needs of the Department

16. The Department is custodian for tens of millions of data records. There is no evidence, outside MOD HQ, with the exception of the specialist personnel agencies, that these large data records are systematically reviewed and cleansed to meet the obligations of the Data Protection Act.

17. Overall security procedures need to be reviewed, simplified, wherever feasible, and accompanied by an invigorated and rigorous audit and compliance regime, led at executive board level. The standard of reporting of losses laptops, PDAs and USB storage devices is inconsistent and unsatisfactory.

18. The loss of four laptops containing 600,000 personal records from unattended vehicles in clear breach of security instructions (and common sense) out of total population of 55 laptops over a period of less than four years indicates a failure of supervision.

19. The effective management of information risks must engage every user, military and civilian, across the Department, and within our community of commercial suppliers. There is an urgent need to review training and education needs and to embed appropriate themes in curricula and training programmes from basic training, through generalist and specialist courses, as 'business as usual'. This is acknowledged in MOD HQ.

20. The Defence Information Infrastructure Future (DII/F) programme will, when completed, provide the IT infrastructure capabilities currently delivered by a range of legacy programmes some (of which TAFMIS is one) retained within Top Level Budget holder (TLB) business areas. These TLB-managed legacy programmes currently retain their own governance mechanisms. The leadership challenge is for these mechanisms to maintain visibility and control of all those legacy systems across the Department until the migration of their infrastructure elements to DII/F has been completed.

21. There is a shortage of expertise across government and private sectors, particularly in accreditors. This constitutes a significant risk to the Department.

22. A serious security event of this nature was inevitable. However, it was clear from all those interviewed that there is an acknowledgment of the need to address these issues jointly and as a matter of priority.

MOD GOOD PRACTICE

23. Notwithstanding the Departmental failings there are a number of examples, both past and current, of MOD good practice.

a. MOD's Director General Information (DG Info) has played a major role over the past 5 years in support of the cross-Government Senior Information Risk Owner (SIRO) network, which has been led by the Cabinet Office. The Department was, therefore, able to respond promptly to the loss of HMRC data in November 2007, and to the subsequent Cabinet Office initiatives.

b. The Department introduced a number of emergency measures in the wake of the data loss on 9 January 2008, which have been effective in preventing similar damaging losses. All laptops without approved full-disk encryption were recalled to secure MOD sites, and a large order was placed by MOD for commercial licences to install the BeCrypt product on as many laptops as possible.

c. The Department has leads for Data Protection policy and enforcement, as well as a network of Data Protection Officers (DPOs). Those organisations within the Department for whom handling of large volumes of personal data is core business have good security, data protection and information risk management procedures.

d. There is evidence that the Department has been galvanised into further useful work. The Vice Chief of Defence Staff (VCDS) is developing an action plan, to produce a new conceptual basis for security, and an assessment of current security vulnerabilities. Front Line Commands are improving their data handling practices and efforts to raise awareness. For example:

(1) HQ FLEET is implementing a roadshow to their sites on Data Protection, to raise awareness.

(2) HQ Land Forces have recently appointed a Chief Information Officer at Brigadier level, to ensure that “all Land Forces personnel using electronic data systems are briefed in succinct and clear terms on their responsibilities for Data Protection, and understand them”.

(3) The RAF has withdrawn laptops from recruiters whose business no longer justifies the accompanying risk.

(4) The Permanent Joint Headquarters (PJHQ) has issued staff guidelines for data protection, interpreting the 8 principles in a ‘user-friendly’ format.

APPROACH

24. Approximately 70 people have been interviewed. Senior stakeholders from all three Services and senior MOD officials have been consulted, to gain an understanding of the strategic direction and policy with regard to the protection of personal data and information risk management. Specialist MOD technical and project-level staff with responsibility for personal data security and systems, and for the auditing of data on releasable media, have also been interviewed. A list of MOD interviewees is provided at Annex B.

25. A series of discussions have also been held with senior private sector managers charged with the management of information risk and personal data security. The purpose of this was to gain an understanding of wider commercial good practices and a statistical baseline against which to compare MOD procedures and loss/theft statistics. This information was provided on a non-attributable basis.

26. Key policy and doctrine documents regarding personal data security have been drawn on, both within the MOD and from wider Government work, including drafts of the developing Cabinet Office Report; as well as emerging data on the extent of MOD’s personal record holdings, the main systems involved in managing and storing these, and the statistics for MOD’s laptops and other portable media holdings and loss/theft statistics.

TERMINOLOGY

27. This report will refer frequently to three distinct, but interrelated, concepts concerning the handling of personal data (and information more generally) – **Security**, **Data Protection**, and **Information Risk Management**. It is, therefore, important to define these.

a. Security. This refers to data handling within the general context of MOD and Government security procedures and practices ie the physical, personnel, procedural and technical measures and regulations in place to ensure the required availability of data, and to protect it against unauthorised disclosure or alteration.

b. Data Protection. MOD has obligations under the 1998 Data Protection Act to ensure that it processes, handles and protects its holdings of personal data with due care. Data Protection therefore refers to the policy and procedures MOD has in place to meet these obligations.

c. Information Risk Management. Information is a key strategic business asset. As such the way in which it is handled and exploited presents both benefits and risks. Information Risk Management refers to the policy, principles and culture within MOD to identify these, and achieve an appropriate balance between the delivered benefits and the residual risks.

28. The approach on how to combine these areas when dealing with personal data differs from organisation to organisation. Some private sector companies, for instance, have fully integrated their Information Risk and IT Security Departments, in recognition of the potential synergies. In contrast, RAF Air Command prefers to keep the Security and Information Assurance areas distinct, albeit with extremely close working relations on the relevant issues. There is no standardised approach and no attempt to prescribe one will be made in this report. Rather, it should be recognised that there are key interdependencies between the three areas identified above.

29. The following glossaries are provided:

- a. Terminology (Annex C)
- b. Abbreviations and acronyms (Annex D)

HISTORICAL CONTEXT

30. The Data Protection Act of July 1998 replaced the 1984 Act. The new Act encompassed electronic records in addition to paper-based data covered by the earlier Act. It also mandated that all Data Controllers handle personal data in accordance with eight key principles, which are set out at Annex E. Work within the MOD to ensure compliance with the Data Protection Act was taken forward by the (then) Directorate General Information and Communications Systems and, subsequently, Directorate Claims and Legal.

31. This work introduced a number of processes and roles to ensure the requirements of the 1998 Act were met by the Department:

- a. All TLBs and Agencies were informed of the need to develop mechanisms to comply with the statutory obligations. Focal points were set up within the organisations and offered draft terms of reference.

- b. A Department Data Protection Officer (DPO) was appointed, with a network of junior DPOs operating across the different areas of the Department. This structure remains in place today and supports over 40 TLBs and Agency DPOs. It receives regular updates to guidance notes and is encouraged to attend annual seminars, which are well attended.
- c. These roles and processes were promulgated by a series of Defence Instructions and guidance notes that were later incorporated in Joint Service Publication 400, which remains (in a revised form) to this day.

32. Since the turn of the millennium, Central Government has driven forward a number of initiatives designed to ensure Government and 'UK plc' in general makes effective and secure use of Information Technology to deliver services and enable national competitiveness in a globalised marketplace. The key documents in this context are:

- a. *"Risk: Improving Government's Capability to Handle Risk and Uncertainty"* produced by the No10 Strategy Unit in November 2002.
- b. *A United Kingdom Government Strategy for Information Assurance* produced by the Cabinet Office in July 2003.
- c. *"Transformational Government Enabled By Technology"* produced by the Cabinet Office in November 2005.
- d. *"A National Information Assurance Strategy"* revised by the Cabinet Office in June 2007.

33. The Department responded to these initiatives through a number of changes to the way in which it does business, particularly with regard to the provision of Human Resource services. The Joint Personal Administration (JPA) system for the military and the People, Pay and Pensions Agency (PPPA) for MOD civilians, for example, hold large quantities of personal data to enable the better delivery of services to individuals.

34. Since 2000, Data Protection procedures within the Department have also struggled to keep up with the pace of these Government-driven changes and perceived priorities. It is understood that the Department's principal focus following the 1998 Data Protection Act concerned facilitating access requests. The proper management and security of data received less attention. For instance, the requirement of the Act to provide 'adequate protection' was open to differing interpretations in the design of complex ICT systems. Additionally, the focus on the introduction of the Freedom of Information Act in 2005 exacerbated the tendency to focus on responses to information requests, rather than the proper management of information.

THE ROWLINSON REVIEW - 2005

35. “In June 2005, against the background provided by the key DII/F programme, the need for increased interoperability and the growing threat, the Departmental SIRO and the Departmental Security Officer (DSO) jointly sponsored the Rowlinson Review, a *“review of the way that Information Assurance (IA) was implemented within the MoD from the generation of its policy to its practical implementation through life, and make recommendations for how MOD’s approach to IA should be improved.”*”.

36. The Review report, issued in December 2005, concluded that a basic structure existed within the Department, which was geared to addressing Information Assurance related issues and that much work had been done to improve matters, particularly in addressing Computer Network Defence (CND), after the Lovegate virus attack in April 2003. However, the Review identified a number of weaknesses which the Department needed to address, including the need to coordinate activity more effectively across the Department.

37. It is understood that a total of 76 specific actions were recommended; 42 of which have been completed. Effective implementation, which is essential, is being jointly overseen by the two senior sponsors in MOD HQ. Work continuing on the remainder will be integrated with actions emerging from the Cabinet Office report and this report. It will be important that the TLBs across the Department support this coordinated programme of work.

STATISTICAL CONTEXT

38. It will be useful here to give some overall statistics, which will set the context in which MOD handling of personal data and releasable media can be considered.

a. MOD holds some 60 million personal records in total (this includes duplicated records).

b. MOD owns an estimated 35,000 laptops, of which some 13,000 currently have full-disk encryption³ capability and 10,000 have a partial-disk encryption⁴ capability. The remaining 12,000 are unencrypted. It should be noted that MOD is currently in the process of ensuring that all but 2,000 of the entire laptop fleet will be equipped with full-disk encryption. (These remaining 2,000 laptops will be taken out of service).

³ Full-disk encryption is a technique in which essentially the entire disk drive is encrypted either by a specific hardware device or by embedded software. This ensures that all user data is encrypted.

⁴ Partial-disk encryption is a technique where individual folders or partitions of the disk drive are encrypted. This approach has the potential disadvantage that the user, either deliberately or accidentally, may store data on the disk in unencrypted form.

c. Lost or stolen MOD-owned laptops numbered 130 in 2007. Out of a total laptop population of 35,000, this represents a loss rate of approximately 0.4%. A comparable figure for industry and the wider population is an annual loss/theft rate of between 1-2%

d. 58 USBs/PDAs that contained MOD data have been recorded as lost or stolen in 2008 so far, set against figures of 78 in 2006, and 22 in 2007⁵. However, there are no firm statistics on total MOD holdings of PDAs, USBs and other mobile data storage devices: the loss/theft rate cannot, therefore, be determined with accuracy.

39. The recording of thefts and losses, particularly within lower-level organisations, is unsatisfactory. This is despite there being a comprehensive policy for Alert, Warning and Response in JSP 541.

⁵ The figures for 2008 may reflect the increased rigour of the reporting process.

PART ONE – THE MAIN CIRCUMSTANCES AND EVENTS THAT LED TO LOSS BY MOD OF PERSONAL DATA ON 9 JANUARY 2008

DISCLAIMER

1. It is understood that the officer involved in the loss of the laptop on 9 January 2008, has been the subject of administrative action. The intention is to set out, as far as is possible, the sequence of events with regard to the Training Administration and Financial Management Information System (TAFMIS) system and attendant procedures and protocols which led up to the loss of data. A full chronology is set out in tabular form at Annex F. This report is not admissible in support of service disciplinary proceedings, and makes no comment on the advisability or otherwise of action in respect of the junior officer involved.

WHAT IS TAFMIS?

2. The TAFMIS provides ICT support for the Army Recruiting and Training Division (ARTD) and for Training Development Teams within the Arms and Services Directorates. The system also supports the Adventurous Training Group in Germany, Regimental Headquarters and Royal Marines. It has also been extended to support recruiting functions of the Royal Navy and the Royal Air Force.

3. TAFMIS is deployed at some 300 locations¹ throughout the UK mainland, Northern Ireland and at a few sites in Germany. There is a total population of 9967 terminals and 562 laptops² supporting different versions of TAFMIS.

| Type | Role | Numbers |
|-----------------------|---|----------------|
| TAFMIS-R ³ | Army Recruiting | 280 |
| TAFMIS-T | Army Training | 144 |
| TAFMIS-R(H) | RN and RAF Recruiting uses Office Automation only | 87 |
| | RN and RAF Recruiting using SQL database | 51 |
| Total | | 562 |

4. Recruiter laptops, which include R and R(H) variants, represent 418 of this fleet. TAFMIS-R devices are deployed in support of Army Recruiting and are allocated between Officer and Soldier recruiting. Officer recruiting involves a long timescale and therefore the system tends to contain more information about candidates. However, officer recruitment involves fewer people (c15,000 soldier records per year, c1,500 officer records). For both Officer and Soldier systems, users only download a small subset of information onto mobile devices at any time. Corps and Regimental HQs can also access officer recruiting data.

¹ TAFMIS System Security Policy Issue 4.0, Doc Ref: C343640/SEC/SSP July 2007

² EDS response to meeting actions arising from meeting with Sir Edmund Burton, 25/3/08

³ An updated version of TAFMIS-R, TAFMIS-RH(A) was bought into service in August 2007.

5. RN/RAF TAFMIS-R(H)⁴ laptops (also known as TRH) account for 138 of these. Some are used solely for Office Automation (OA) and have not had personal data records downloaded from the TRH database. 51 are used primarily for RN and RAF recruiting and have had SQL database installed: this database stores a complete copy of the main TRH database. There are also 300 PDAs,⁵ which can access, retrieve and, potentially, store TAFMIS data.

6. This review concentrates on the 51 TAFMIS-R(H) laptops using the SQL database. The numbers of these laptops assigned to the RN and RAF are 28 and 23 respectively. Since January 2008 the RAF have withdrawn their recruiter laptops, having concluded that they do not need to carry mobile devices.

Recommendation 1: RN to undertake a review of their recruiter process and, in particular, the need to use mobile devices holding a complete copy of the recruiter database.

TAFMIS SPONSORSHIP AND ACCREDITATION

7. TAFMIS came into service prior to the creation of Defence Security Standards Organisation (DSSO). Accreditation⁶ was, therefore, the responsibility of the Adjutant General (AG), the Top Level Budget Holder (TLB). DSSO was formed in April 2001 to take on accreditation responsibilities and Defence Council Instruction (DCI) Joint Services 143/04 provided a mechanism to transfer this responsibility and resources from TLBs. Since Army TLBs were not able to hand over relevant resources, DSSO was unable to take immediate control and provide accreditation responsibilities, so DSSO began a phased transition of LAND projects. However, as DSSO saw TAFMIS as a mature system, it was agreed that the AG TLB should continue to accredit the system.

TAFMIS HISTORY- SUMMARY

1996

October - PFI agreement with Prime Contractor EDS (10 year contract), sponsored by Army Training and Recruiting Agency (ATRA).

1997

September - TAFMIS in service date, providing support for Army Training Development with a contract extension to August 2007.

⁴ Questionnaire notes from MOD ARTD MIS Feb 08.

⁵ DSSO Accreditation Review of the TAFMIS, DSSO/01-03-05 4 Feb 08.

⁶ Security accreditation is a mandatory MOD requirement for all IT-based systems that electronically store, process or forward official information. It is the process through which it is confirmed that the use of these systems does not pose an unacceptable risk to National Security and the Data Protection Act.

1999

- January - TAFMIS training support capability extended to provide support to the Army for Recruiting (TAFMIS-R).

2002

- January - Army recruiting functionality was extended to meet requirements of RN and RAF. This project known as TAFMIS Recruiting (Harmonised) - (TAFMIS-R(H)), was initially run by Armed Forces Pay and Administration Agency (AFPAA) as a separate contract.

2003

- January - MOD issued directive Defence Council Instruction (DCI) General 23/03, all new laptops to be encrypted from April 2003. In-service laptops to be encrypted by January 2006.
- January - ATRA informs EDS⁷ of DCI General 23/03 and ATRA policy to use DataVault encryption solution.
- February - MOD Security updated Joint Service Publication (JSP) 440 to reflect DCI 23/03, but poor wording allows misinterpretation of encryption implementation dates.

2004

- April - Adjutant General Information Management Security Officer (AGIS SO2 Info Man Sy) confirms that ATRA could issue new laptops unencrypted, as long as encryption is installed before January 2006.
- July - EDS was given formal instruction to install suitable encryption mechanism via Contract Management Note (CMN) 2548.
- August - RN TAFMIS-R(H) laptop stolen from vehicle in Bristol which belonged to the Manchester Armed Forces Careers Office (AFCO).

2005

- December - Confidence testing highlights synchronisation difficulties between DataVault encryption and SQL Database on TAFMIS-R(H) laptops.
 - Two Army TAFMIS-R recruiting laptops stolen from Edinburgh Armed Forces Careers Office (AFCO)⁸.

2006

- January - Date by which all MOD laptops should be encrypted.
- March - EDS report that encryption instructions will be issued at installation time. (Note: All TAFMIS laptops have been in breach of MOD JSP 440 security instructions since January 2006).

⁷ D/ATRA/2203(MIS) dated 29 January 2003, Cryptographic Protection of Information held on Laptop and Notebook Computers.

⁸ One of these held approximately 500 personnel records and the other held nil.

- April - JSP 440 extends encryption deadline to 1 January 2009 for laptops purchased before April 2003.
- May - EDS report encryption installation is 96% complete for TAFMIS-T and TAFMIS-R laptops. Encryption solution for TAFMIS-R(H) laptops with SQL database still in development and test.
- June - ATRA changes name to Army Recruiting and Training Division (ARTD).
- July - TAFMIS-R(H) RAF laptop belonging to the Leeds AFCCO stolen from car outside private residence.
- August - At change management monthly meeting it was reported that encryption roll-out was complete⁹, but 55 TAFMIS-R(H) laptops were not working. **Reporting then ceases within EDS and ARTD without explanation**
- September - MOD Security issue Defence Instruction Notice (DIN) (2006DIN08-020), which provided clarification for encryption deadline waiver announced in JSP 440 Issue 3.5 (April 2006). Encryption policy now extended to January 2009 for all laptops purchased before 1 January 2006, but requires Principal Security Advisor approval, if being replaced by Defence Information Infrastructure (DII) programme. No such approval was sought by ARTD.
- 2007
- October - TAFMIS-R(H) RN laptop stolen from car in Manchester.
- August - Responsibility for TAFMIS-R(H) applications transferred to ARTD MIS from Service Personnel and Veterans Agency (SPVA), formerly known as AFPAA. ARTD remained responsible for infrastructure.
- 2008
- January 9/10 - TAFMIS-R(H) RN laptop stolen from car in Birmingham.
- 18 - All recalled TAFMIS laptops secured on MOD sites.
- 21 - Secretary of State provides oral statement to Parliament.
- 21 - New rules announced on accreditation and laptop encryption.
- 28 - EDS reaffirms that TAFMIS-R(H) laptops contain no data entries dating earlier than 1997.

⁹ 20080201-Security of TAFMIS Laptops-Narrative Version 1 2-U (2).doc. Restricted.

February 1 - EDS informs MOD that earliest personal record on TAFMIS data base is 1977 rather than 1997.

- MOD Security mandates (2008DIN02-002) that all laptops are to have approved full disc encryption installed, if device is to be taken off an MOD site.

5 - 2nd PUS/VCDS notifies key stakeholders of Sir Edmund Burton's review.

April 30 - Review report submitted to PUS MOD.

2009

November - Expected expiry of TAFMIS service contract.

TAFMIS PROGRAMME GOVERNANCE

7. The governance of the TAFMIS programme, which involves a major prime contractor and users from all three services, was unclear. At Annex G is a copy of TAFMIS Programme Governance, taken from the TAFMIS Security Operating Procedures. A simplified diagram is offered by ARTD at Annex H.

TAFMIS HISTORY-DETAILED

8. The original TAFMIS requirement (c.1996) did not require laptops to have disc encryption, as the system operated at System High Restricted. (Only systems classified Confidential and above required encryption). In 2001 laptops that were to be used in Northern Ireland had the DataVault encryption product installed.

9. In January 2003 MOD changed its laptop security policy dictating that all laptops procured after April 2003 should incorporate an approved encryption product. Existing laptops (purchased pre April 2003) were to incorporate an approved encryption product by 1 January 2006. It should be noted that the laptop stolen in Birmingham on 8 January 2008 was purchased on 9 December 2002.

10. In January 2003 ATRA notified EDS of MOD's new security requirements and deadlines, ATRA policy to use DataVault and the implication that had on TAFMIS laptops. A Contract Management Note (CMN 2548) was subsequently issued in July 2004 to install a suitable encryption mechanism.

11. In April 2004 the Adjutant General Information Management Security Officer confirmed that ATRA could issue new unencrypted TAFMIS laptops to users, providing DataVault was installed before January 2006. This contradicted the direction of the MOD Director of Defence Security (DDefSy), that all new laptops had to be encrypted from April 2003. It has been suggested that ambiguities in writing related paragraphs in DCI General 23/03 and MOD Security Joint Service Publication (JSP) 440, could have caused confusion when interpreting MOD laptop encryption policy.

Note. The intent of the MOD instruction to ATRA in January 2003 was clear, as ATRA conveyed the correct message to EDS in their Policy letter of January 2003. However, it cannot be established why ATRA then chose a different interpretation of JSP 440 to allow new laptops to be issued without encryption.

12. Originally an encryption upgrade was going to be installed as part of a technology refresh in 2005. However, encryption key code delivery problems meant that encryption had to be completed as a separate project. Also it was noted in the September 2005 Change Management Note (CMN) review meeting that there were minor issues with TAFMIS-R(H) laptops that needed resolution. Details of the exact issue were not recorded. The technical solution was finally agreed in September 2005 and MOD (ATRA) accreditation was reportedly provided around September/October 2005, although no records can be located to confirm this.

Recommendation 2: MOD to ensure that all employees and contractors understand what key information and documents must be maintained as records, and to highlight consequences of failing to do so.

13. ATRA authorised EDS to begin implementation in January 2006, but it had been recognised earlier (in December 2005) that there were SQL database synchronisation issues with TAFMIS-R(H) laptops. This was judged to require the development of an applications fix to enable the DataVault encryption and TAFMIS-R(H) SQL database to function properly. In March 2006 user instructions on how to use DataVault were completed and issued just prior to encryption installation on the non-SQL laptops that formed the majority of the TAFMIS 'fleet'. A copy of these instructions can be found at Annex I.

14. It was evident from discussions with TAFMIS service staffs that they believed that all TAFMIS laptops had been encrypted. Reading the user DataVault instructions that were sent out to all TAFMIS users, it is clear why this belief was held: the opening paragraph states that all TAFMIS laptops were being encrypted.

“Extract from DataVault instructions”

IMPORTANT for the Attention of (The Vault Owner),

Over the next few weeks we will be remotely installing Reflex Data Vault, a hard disk encryption solution to all laptops within TAFMIS using either SMS or VNC. Reflex Data Vault will create a secure encrypted drive on the user's laptop that will be used for storing all information at **RESTRICTED** level and above. After installation has completed you will notice a new drive within 'My Computer' and 'Windows Explorer' G:.

15. In April 2006 MOD Security released JSP 440 Issue 3.5, which changed the date by which all laptops should be encrypted from 1 January 2006 to 1 January 2009.

16. In May 2006 EDS informed ATRA that approximately 96% of TAFMIS-R and TAFMIS-T laptops had successfully been installed with DataVault encryption and 34% of TAFMIS-R(H) laptops had DataVault installed. However, the synchronisation solution for the TAFMIS-R(H) SQL laptop, which held the large personnel database, was still in development and test, involving a population of 51 SQL laptops.

Conclusion From the original laptop encryption compliance date 1 January 2006 to 1 April 2006, the unencrypted TAFMIS laptops were in breach of MOD laptop encryption policy. This deadline was formally extended in April 2006 by JSP 440 Issue 3.5 to achieve laptop encryption by 1 January 2009.

17. Laptop encryption reporting was covered at two joint EDS and ATRA meetings:

- a. Service Delivery Meeting (fortnightly)
- b. Change Management Note Meeting (monthly)

18. Due to changes of ATRA Service Managers and associated meeting responsibilities in 2006, ATRA and EDS agreed to close the encryption reporting at the Service Delivery Meeting and move all reporting to the CMN Meeting.

19. In June 2006, following the Defence Training Review, ATRA lost its agency status and was renamed ARTD.

20. In July 2006 an RAF TAFMIS-R(H) laptop was stolen from a car in Leeds which belonged to the Armed Forces Career Office (AFCO) in Bristol. No disciplinary action was taken against the individual who lost the laptop. This loss was in breach of the then extant policy on laptop encryption and was not notified to Ministers.

21. At the CMN monthly meeting in August 2006 it was reported that the DataVault rollout was complete, but that 55 TAFMIS-R(H) laptops were not working. No other information is provided about the specific problem. Reporting of the DataVault encryption upgrade then ceased, without explanation, with no formal record of closure. Neither ARTD (formerly ATRA) nor EDS have an explanation of why the encryption action was dropped.

22. In September 2006 an MOD directive (DIN 2006DIN08-020) was issued to clarify laptop encryption policy. It stated that any unencrypted laptop purchased before 1 January 2006 required approval from the Principal Security Advisor, if it was being replaced or refreshed by the DII programme (see Annex J), or it had to install an approved Defence Infosec Product Co-Operation Group (DIPCOG) approved encryption product as soon as possible and before January 2009.

23. In July 2007 MOD Security released JSP 440 Issue 3.6, which dropped the requirement announced in DIN 2006DIN08-020 to seek approval from the Principal Security Advisor.

Note. TAFMIS laptops that were not encrypted would have been in breach of security instruction from September 2006 to July 2007 because no such request for approval was sought by ATRA, who believed all TAFMIS laptops were encrypted, although there is no evidence to support such an assumption.

24. When JSP 440 Issue 3.6 was released in July 2007 it meant TAFMIS laptops that were previously in breach of security procedures would be compliant until 1 January 2009, providing laptops had been purchased before 1 Jan 06.

25. During the night of 9/10 January 2008, the TAFMIS-R(H) laptop of an RN recruiter was stolen from the boot of his car, parked in Edgbaston, Birmingham.

Conclusion: At the time the laptop was stolen on the night of 9/10 January 2008, although the user was in clear breach of physical security rules, it did not break any security rules relating to laptop encryption. However, there were two definite periods (from Jan 06 to Apr 06 and Sep 06 to Jul 07) when TAFMIS-R(H) laptops were being used in breach of MOD laptop encryption security policy. Indeed, the RN laptop stolen in October 2006, which contained the same dataset as that lost in January 2008, was in breach of the extant policy.

| Year | Total No: lost/stolen TAFMIS laptops | TAFMIS-R(H) Using SQL | TAFMIS-R(H) OA Not using SQL | TAFMIS-R | TAFMIS-T | TAFMIS Unknown |
|------|--------------------------------------|-----------------------|------------------------------|----------|----------|----------------|
| 2008 | 1 | 1 | 0 | 0 | 0 | 0 |
| 2007 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2006 | 4 | 2 | 1 | 0 | 1 | 0 |
| 2005 | 4 | 0 | 1 | 2 | 0 | 1 |
| 2004 | 1 | 1 | 0 | 0 | 0 | 0 |
| 2003 | 0 | 0 | 0 | 0 | 0 | 0 |

26. Of the 562 TAFMIS laptops thought to have been fitted with an encryption product, (except the 51 RN/RAF TAFMIS-R(H) laptops with SQL), ARTD MIS confirmed on 7 March 2008 that it appears that none of the TAFMIS-R(H) SQL laptops had data encrypted on them. Subsequent analysis of the laptops has shown that the encryption product was not fully installed or operational as believed by ATRA, ARTD, RN and RAF staffs. All TAFMIS-R(H) laptops with SQL that were stolen were taken from parked cars. The clear instructions forbidding users to leave laptops in unattended vehicles was not being observed.

Recommendation 3: Supervising officers to be rigorous in enforcement of security instructions.

Note. Since the incident of 9/10 January 2008 all TAFMIS laptops, including TAFMIS-R(H) laptops currently in use outside secure MOD sites, have had BeCrypt full disk encryption installed. The remainder are held within secure MOD sites. The intent is to encrypt all TAFMIS laptops and this process is ongoing.

DATA PROTECTION

27. The laptop stolen from Edgbaston in January 2008 was a TAFMIS-R(H) laptop using SQL, which contained the whole RN/RAF database, holding some 600,000 personal data records. Although the laptop held records relating to some 600,000 recruits or potential recruits, investigations by MOD DG Info staff, in conjunction with EDS, has indicated that the database includes personal details of some 400,000 additional individuals, who were either referees or parents of the recruits. Technically, therefore, the laptop held some 1,000,000 personal records. The reason for the large number of records is due to the original user requirement and design drawn up between RN, RAF and AFPAA. The TAFMIS-R(H) design synchronises the whole database from the main server to the laptop.

Note. It appears that the original RN/RAF recruiter requirement was for a portable copy of a database comprising several hundreds of thousand records. Although the review team has found evidence of the initiation of the TAFMIS-R(H) disk encryption task, there are some significant gaps in the available evidence:

- **No trace of the initial requirement.**
- **No evidence of the approval process for the need for the major RN/RAF database.**
- **No evidence showing completion or acceptance of TAFMIS-R(H) SQL encryption process.**
- **No written evidence that the officer whose laptop was stolen had signed the mandatory notice appended to the System Security Operating Procedures.**
- **No evidence that the system for administering the security instructions was enforced, either by the user or contractor, although the process was designed to control access to and use of the system.**

Conclusion. The standard of project management on both sides of the MOD Customer/EDS Contractor interface was poor. Despite the high number of change requests, both project managers should have identified the significance of the encryption task, accorded it appropriate priority, and ensured that progress was hastened and recorded rigorously.

Recommendation 4: It has not been possible to locate evidence that would support formal disciplinary action. However, it is recommended that the senior leadership in ARTD and in EDS should review the project management processes and procedures, taking appropriate remedial action.

28. It is understood that initial proposals provided by EDS were for small subsets of information to be carried on mobile devices. This did not meet the RN/RAF user requirement, which was for RN/RAF mobile users to have a complete version of the main database. Alternatives were discussed, that would have allowed connection to a central server, but communications costs would have been prohibitively expensive in 2002.

29. MOD issued instructions on Data Protection responsibilities in February 2001 and updated lists of MOD Data Protection Officers in July 2001 and periodically thereafter. However, the legal position of the TAFMIS-R(H) database does not appear to have been questioned. There is no evidence that any of the key stakeholders (EDS, AFPAA, ATRA, ARTD, RN or RAF) raised concerns that the TAFMIS-R(H) design would breach data protection principles.

30. As stated above, MOD Data Protection Act 1998 (DPA 1998) guidance is located on the Defence Intranet and contains a substantial amount of guidance for DPA practitioners and other MOD staffs. It provides points of contact across the whole of MOD, including training and recruitment organisations in the RN, Army and RAF. It is noted that the Army ARTD Data Protection Officer (DPO) is also the project manager for the TAFMIS system. A copy of the MOD DPO structure and terms of reference can be seen at Annex K.

31. MOD DPA Guidance Note No:5 'MOD Retention Policy' provides an extensive list of data types and retention periods, including retention periods for hardcopy material. However, it is not clear in defining how long electronic records are to be kept for Armed Forces and Civilian recruitment. It is also noted that there is a significant unexplained difference in retention periods for unsuccessful candidate data between Armed Forces (7 years) and Civilians (1 year).

Note. Discussions with MOD DPA team highlighted the fact that the 'Limitation Act for Armed Forces' means that Armed Forces recruitment data needs to be kept for longer than equivalent Civilian records.

Recommendation 5: MOD to review DPA retention policy to remove potential ambiguities and ensure clarity where variations exist.

32. It is understood that EDS did seek to update the TAFMIS contract in 2005 to reflect DPA 1998 requirements. These had been introduced since the original PFI Agreement¹⁰, which referenced DPA 1984. In particular, it addressed obligations under the seventh principle to keep data secure, but ARTD rejected these amendments on the grounds that it placed a disproportionate responsibility onto MOD. They concluded that the existing contract clause sufficiently obliged both parties to meet their respective DPA responsibilities.

33. The TAFMIS Security Operating Procedures¹¹ (SOPs) cite the DPA 1998 as a reference. A one page guide is provided at Annex C of the SOPs for users. The annex, although providing some useful information, including who to contact, does not list all the major principles of DPA and provides inadequate guidance to the user on how to ensure compliance, (i.e. how long a document or record should be kept). Neither does the guide highlight the MOD's repository of DPA guidance on the Defence Intranet.

¹⁰ TAFMIS Development and Service Provision Agreement, PRT 141/496 S18v14I

¹¹ TAFMIS Security Operating Procedures Issue 4.0, Doc Ref: C343640/SYOPS July 2007

34. During a visit to an Armed Forces Career Office (AFCO) Joint Services recruiting unit in London, it was discovered that recruiting staff were unaware of MOD DPA retention policy for recruiting data. Nevertheless, the TAFMIS system does not allow recruiters to delete information once submitted to the database. The only people able to delete are EDS staff under authorisation from ARTD. Yet it is understood that no policy or process currently exists to manage data according to the eight principles defined within the DPA 1998.

Recommendation 6: Where MOD or an MOD contractor provides data management services, there should be an agreement between the relevant parties detailing responsibilities with reference to MOD's DPA record retention policy for personal data types.

Recommendation 7: Contractor to be tasked to cleanse TAFMIS data base as a matter of urgency.

35. It was also noted that standard declaration and check procedures detailed within the TAFMIS Security Operating Procedures (Sy Ops) were not being implemented. No one could produce a signed user declaration that the Sy Ops had been read, either by the user, Site System Security Officer or TAFMIS Manager. It is understood that all TAFMIS users were emailed on 22 January 2008 to remind them of their security (JSP440) and TAFMIS Sy Ops responsibilities. ARTD MIS Branch and EDS are currently seeking a technical solution to prevent users accessing TAFMIS without first having signed the Sy Ops.

Recommendation 8: MOD to show greater rigour in ensuring that system security procedures are enforced.

Recommendation 9: MOD to ensure that individual and corporate responsibilities under DPA 1998 are understood and complied with.

PART TWO – MOD PROTECTION AND MANAGEMENT OF PERSONAL DATA

OVERVIEW

1. The risk of a loss of data on the scale which took place on 9 January 2008 was not identified on any of the relevant organisations' risk registers. Nor was mitigation in place to prevent it. The major impact of this event was an inevitable outcome of a series of failings in governance, process and leadership.

CONTEXT

2. All Government departments operate in an environment of rapid technological change, which presents both opportunities and threats. For MOD, significant developments include:

a. Culture Changes – the 'Facebook Generation'. The Department recruits from, and exists within, a culture where the rapid and often uninhibited exchange of information is the norm. At work, this behaviour must be tempered by common sense and sound judgement, informed by data protection practice, and the particular concerns of MOD work. However, returning to strict information control of the type applied to paper documentation of fifteen or more years ago is not considered practical in the modern working and cultural environment.

b. New Ways of Working. The Department has sought to capitalise on these technological and cultural developments by adopting modern ways of working, particularly as regards data exchange and access. Examples are the creation of the Human Resources Management System (HRMS) and JPA systems, allowing individual users better access to their personal data, and enabling the improved delivery of personnel services. The Department is also adopting a risk management approach to its business, although this has not yet addressed at Board level the domain of information risk. However, this is now a well-developed process for the SIRO to rule on individual risk-balance cases.

c. Decline in Security. One consequence of embracing this new data-sharing culture has been a decline in overall Departmental security practice. The evidence for this is mainly anecdotal, but a considerable number of senior officials concurred on this point. They shared a concern that the younger generation of MOD staff are not inculcated with the same culture of protecting information as their counterparts from previous generations.

d. Resourcing Security. There are resource implications in achieving effective security, particularly in accreditation, audit and compliance. Pressures to reduce staff numbers across the Department are already presenting significant risks. For example, the Department has a significant shortage of accreditors, who are crucial to the validation of security measures in ICT systems.

e. Accounting for Computers and USB Devices. The standard of accounting for laptops, PDAs and USB devices, and reporting losses, is poor and prevents effective management and security of devices and their data. See also Paragraph 16.

Recommendation 10: That all MOD organisations and business units report thefts and losses of removable media in strict accordance with JSP541.

f. 'Need to Know' vs 'Need to Share'. The cumulative effect of these developments has been to create a tension between the traditional MOD 'need to know' principle for security, and the modern 'need to share' assumption as regards data. The benefits of new ways of working, and the ever-increasing rate of technological change, mean it is impractical to return to a strict 'need to know' culture. However, recent incidents suggest that unmanaged 'need to share' practices lead to unacceptable vulnerabilities. Staff procedures must be reviewed and adapted to gain the benefits offered by new ICT and communications technology, while addressing the attendant information risks.

Recommendation 11: MOD to review and adapt established staff procedures and processes, taking account of the opportunities and vulnerabilities implicit in new ICT.

HOW MUCH PERSONAL DATA DOES MOD HOLD, AND WHY?

3. Protection of personal data is not simply a matter of the security and risk management procedures applied to its handling. As a general principle, the more information an organisation holds, the harder it will be to protect it. The evidence suggests that the Department holds a very considerable amount of personal data (some 60 million personal records, much of it duplicated), without a clear business case for doing so on such a scale.

Recommendation 12: MOD to carry out a full audit of its total personal data holdings, based on the work already completed as part of compliance with the Cabinet Office review.

4. The Department is not good at limiting and cleansing its personal data holdings. There are a number of reasons for this:

a. The cost of deletion is greater than the cost of storage.

b. Failure to consider the legal implications and risks accompanying user requirements for large quantities of data on removable storage devices. It is understood that the scale of personal data held on the RN/RAF TAFMIS laptops was attributable to the user requirement. There is no evidence that the legal implications and risks were considered, either by the user community, or by the contractor.

c. Data Protection Officers are not fulfilling their responsibilities.

d. Audit and compliance functions are not being exercised or overseen effectively at board level.

e. Data is replicated without due consideration. This can range from individuals saving duplicate copies of shared area files within their own personal drives, to large scale data replication eg the monthly transfer of data from SPVA to Defence Analytical Services Agency (DASA).

Recommendation 13: MOD to introduce policy and procedures for both data cleansing and data governance, in order to ensure that boards understand the nature and scale of their data holdings and instigate appropriate audit and compliance measures.

f. MOD Centre and senior officials' requirements for ready access to large amounts of data. This was a recurrent and highly significant theme throughout the review. It is widely felt that MOD Centre requirements for briefing and for accurate (and often historical) data to support public statements, responses to Parliamentary Questions, Freedom of Information requests etc necessitated holding large amounts of data over an extended period of time. Clearly, MOD has statutory and constitutional obligations to provide answers to inquiries of this nature with the fullest available information. Nonetheless, it was felt that the Centre's requirement for detailed information creates difficulties for the Department in terms of holding and managing a reasonable quantity of personal data.

Recommendation 14: MOD to carry out a risk-benefit analysis on the requirement to hold large amounts of personal data to meet Centre tasking.

WHAT DOES MOD DO WELL?

5. There are several areas in which the Department has already introduced good procedures, both before and after 9 January 2008.

a. MOD has been, consistently, one of the most proactive Departments in engaging with the cross-Government SIRO network. DSSO audits have revealed an upward trend in MOD data security over the past 5 years.

b. The Department has benefited from an experienced and authoritative SIRO, whose advice and support has been used by the Cabinet Office extensively since the launch of the initial National Information Assurance Strategy in 2003. His expertise has been applied to the evolution of the DII programme, which will replace a range of legacy systems across the Department.

c. Following the loss of HMRC data in November 2007, MOD anticipated the need to address any similar departmental risks and put in place work to address it. This has since dovetailed into the Department's response to the Cabinet Office review. The TAFMIS issues were not picked up on the first round of data collection in support of the Cabinet Office review. This was mainly because LAND would not have identified TAFMIS as a system with specific security concerns as, as far as they were concerned, it was fully accredited and compliant with policy. Moreover, the search was focussed at the time on areas of risk such as bulk data transfer. Whilst holding bulk data on a laptop resulted in the same risks as data transfer mechanism it was actually a feature of the design and again, was not declared.

d. Following the 9 January 2008 incident, the MOD HQ imposed a series of emergency measures. All laptops without full-disk encryption (for example, through the CESG-approved BeCrypt product) were recalled to secure MOD sites, and a large order was placed through the DG Info for commercial licences to install BeCrypt on as many laptops as possible. From the information gained in this review, it appears that all the departmental TLBs have fully complied with these directives. This prompt and effective response, and the efficiency of TLBs in implementing it, is to be commended. However, several stakeholders pointed out that this measure degraded their business capability significantly.

e. The VCDS is developing an action plan, which will produce a revised conceptual basis for security, an assessment of modern security vulnerabilities, and a Training Needs Analysis to help fill the security awareness gap. See paragraph 41 below for more details.

f. Data Protection. There are elements of good data protection practice within the Department. PJHQ provides data protection policy guidance, which enshrines the principle of only holding the minimum amount of data necessary. It also provides a checklist for data handling drawn from the eight principles of data protection within the DPA 1998. MOD HQ has recently moved to create a dedicated lead for compliance with information security and data protection enforcement (distinct from the predominantly Data Protection policy role of the MOD's Data Protection Officer). The 2008/9 editions of the Service Delivery Agreements between MOD HQ and the Departmental TLBs will include an expanded section on data handling responsibilities.

g. Personnel Agencies. It was noted that those parts of MOD for which handling of large volumes of personal data is core business (for instance, SPVA and the Defence Vetting Agency (DVA)) have good security, data protection and information risk management procedures. These constitute good practice.

h. RN. HQ FLEET is implementing a roadshow to their sites on Data Protection, along similar lines to roadshows on raising Drug and Alcohol risk awareness.

i. HQ Land Forces. Other areas have also been proactive. HQ Land Forces have recently appointed a Chief Information Officer at Brigadier level, to ensure that “all Land Forces personnel using electronic data systems are briefed in succinct and clear terms on their responsibilities for Data Protection, and understand them”. The Adjutant General has tasked the Army Inspectorate with auditing whether the Land Forces plans for better information risk management and data protection are carried through (similar to the function it performs for other issues e.g. implementation of the Blake reports).

j. RAF. The RAF has withdrawn laptops from users whose business no longer justifies the accompanying risk.

Recommendation 15: That MOD identifies and facilitates the sharing of good practices.

6. Maintenance of Momentum. The recent data losses have galvanised the Department and its constituent commands and business entities into action. The key now is to ensure that this activity is coherent and engages leaders and users at all levels.

AWARENESS OF INFORMATION AS A KEY BUSINESS/OPERATIONAL ASSET

7. British Defence Doctrine embodies the ‘Manoeuvrist Approach’ to operations, in which key features are momentum and achieving a superior operational tempo. Information is stated to be one of the seven fundamental defence capabilities required by the UK to deliver ‘fighting power’. This demands the effective acquisition, collation, processing, management and distribution of trustworthy information. This key capability holds good across the home base and for operational theatres, within and across boundaries with private sector partners. Indeed, increasing interdependence with private sector partners, coalition partners, and allies, obliges the defence community to address these issues in a joint, national, and international fashion. This capability calls for all users at every level to understand the reasons underlying and to comply with rules and procedures relating to data and information.

8. It is a truism that people cannot manage, effectively, what they do not understand. With very few exceptions, there is little awareness or understanding of the crucial importance of data and information as a critical business asset across the Defence community. Consequently, the Department can have little confidence that it is being exploited to deliver the potential operational benefits, or protected to preserve UK’s defence capability and resilience. There is a need for a body of knowledge to inform understanding.

Recommendation 16: A doctrine for Information Exploitation and Protection to be developed in order to set out the principles by which the UK’s defence forces will deliver the Information capability underpinning British Defence Doctrine.

9. With a few exceptions, Information Risk is not dealt with as a defined risk area on Executive Boards across the MOD community; nor do Audit Committees specifically consider it. There is no mandated assurance or self-assessment process for Information Risk comparable with, for example, those which exist for Health and Safety, Equality and Diversity. Neither is Information Risk addressed within Capability Reviews, although the effective exploitation and protection of information and data are critical business capabilities.

Recommendation 17: A coherent, Joint Service and Civil Service, awareness campaign to be launched to highlight the importance of information and data as a key operational and business asset, with appropriate attention devoted to exploitation and protection, within the law.

Recommendation 18: Information Risk to be addressed as a standing risk item on all Executive Boards and Audit Committees.

Recommendation 19: Mandated assurance processes analogous to those for Health and Safety to be introduced for Information Risk.

Recommendation 20: Information Risk to be formally assessed in Capability Reviews and in Office of Government Commerce (OGC) Gateway Reviews.

DATA PROTECTION

10. It seems likely that the TAFMIS database, comprising over 600,000 personal records, was in breach of the following Data Protection Act principles:

- a. Personal data shall be processed fairly and lawfully
- b. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- c. Personal data shall be accurate and, where necessary, kept up to date.
- d. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- e. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. [Note: this applies to the past storage of the TAFMIS database on unencrypted laptops].

11. However, the principles are not precise: they require judgement. The Department will need to seek guidance on the exercise of that judgement from the Information Commissioner.

12. The data protection issue was not recognised or queried within the MOD user community (which defined the statement of user need) or by the service provider.

Recommendation 21: MOD to seek guidance from the Information Commissioner on the status of the TAFMIS database(s) as regards the Data Protection Act.

Recommendation 22: MOD to ensure that the governance processes for legacy programmes, and project approval and acceptance into service, take account both of the legal requirements of the Data Protection Act and of security accreditation.

13. It is noted that work is in hand to rectify this situation. MOD now has two Head Data Protection Officers, one for policy formulation and one for enforcing and auditing compliance. There is also a structured network of the 43 Data Protection Officers to facilitate co-operation and information sharing. Data Protection obligations are also set out in the Service Delivery Agreements with each TLB. MOD Departmental Structure for Implementation and Compliance with DPA 1998 is set out at Annex K.

14. However, there are still gaps in implementation. Detailed accountabilities for Data Protection across the Department are not yet adequately understood. Beyond the expert community there is little evidence of awareness of the Data Protection Act or its implications for the chain of command; these include the need for appropriate training.

Recommendation 23: Detailed accountabilities for Data Protection across the Department to be clearly articulated.

Recommendation 24: MOD to improve awareness and uptake of current Data Protection Act training.

MANAGING THE DATA ENVIRONMENT

15. Critical Information Requirements. There is an established discipline in the defence community whereby commanders dictate their critical information requirements. This process ensures that resources are concentrated on gathering and collating those elements of information that will meet the commanders' needs. However, the same discipline is not evident in 'business as usual' outside operational theatres. Time and resources are, therefore, wasted gathering and storing information and data that are unlikely to deliver an operational or business benefit. Such superfluous data presents avoidable costs and risks, as in the case of the TAFMIS data base.

16. Remote Access to Data. There is clear evidence of increased awareness of the risks inherent in carrying large volumes of data outside secure premises. For example, the RAF recruiting teams no longer use laptops bearing the TAFMIS database. The business need has evolved to seeking mobile access to data from centrally held and managed databases. This development is to be welcomed, as long as the following conditions are met:

- a. The remote access is truly secure.

- b. There are strict controls on the onward copying and storing on any data accessed or downloaded remotely from these central sources.
- c. The central holdings of the data are appropriately secured and backed-up.
- d. User training and implementation of security procedures are rigorous.

Recommendation 25: That the Department supports initiatives making personal data accessible through secure links to central servers, on the basis that clear guidelines are in place for onward storage of this data, and the system itself is both secure and has adequate redundancy.

17. Sharing Data with Commercial Partners and Third Parties: Sharing data presents other issues. For example :

- a. Some TLBs and Agencies noted that their core business depends on the ability to share data with key industry partners and other third parties. In some cases, there was a lack of clear understanding on what data could be sent over, for example, the Government Secure Intranet, MOD systems themselves, or the internet; and the ability of recipient organisations to receive MOD personal data in a secured/ encrypted fashion.
- b. A number of TLBs work with commercial partners to deliver key services, such as training. In these cases the data protection and management aspects are covered only through standard clauses in MOD Commercial Contracts. These should be revisited to ensure that they are comprehensive.
- c. A number of MOD contractors have access to large amounts of MOD employee personal data, without the requirement to be security cleared. This is because security clearance is only required to handle material marked Restricted and above, a classification which does not currently apply to personal data (though this may change under the Cabinet Office review recommendations).

Recommendation 26: MOD to produce clear policy on sharing personal data with third parties, including changes to standard contractual clauses as required.

18. Use of non-laptop mobile media devices: The Departmental response to recent data loss incidents have focused largely on laptops, but there remains a lack of certainty on how many PDAs/ memory sticks/ other removable media are used to carry personal data or business information and how many of these there are. PDAs are reaching the point where they have the same processing power and storage potential as laptops, yet there are no measures in place within the Department to audit their use. This presents a risk.

19. Although the Department's response to the HMRC incident revealed no CD or DVD data vulnerabilities of a similar scale, there remains a risk of data loss through these media, particularly through staff downloading data to take off-site.

Recommendation 27: To instigate a full census of non-laptop removable media device holdings, in order to ensure that they are formally approved and accounted for on a routine basis.

Recommendation 28: MOD to implement guidelines on the storage of personal data on these devices, including the requirement for encryption, as necessary.

20. Use of private mobile media devices. Evidence suggests that staff use private mobile media devices to process MOD data. It is difficult to determine how widespread this is, and how much it relates to aggregated personal data. However, clear guidelines and regulations on such use need to be reinforced.

Recommendation 29: MOD to reiterate, or revise, Departmental guidance on the use of private mobile media devices to process MOD data.

CREATING A CIO/SIRO NETWORK

21. The role of the Chief Information Officer (CIO) may be considered to be beyond the scope of this review. However, a number of senior stakeholders saw an important role for an MOD CIO, with explicit authority. Those outside MOD HQ, in particular, felt that this post would provide a source of guidance, real authority and accountability that had, hitherto, been lacking.

22. This issue is addressed by the recent Cabinet Office directive that all departments were to name a board member as SIRO. The directive explained that the SIRO, who is an executive familiar with information risks and the organisation's response, may also be the CIO, if the latter is on the board. They own the information risk policy and risk assessment, act as an advocate for information risk on the board and in internal discussions, and provide written evidence to the Accounting Officer on the content of the Statement on Internal Control relating to information risk.

23. It is understood that the Defence Board has two champions for Information Risk Management (2nd PUS and the VCDS). Jointly, they fulfil, at board level the roles set out by the Cabinet Office. The organisation that fulfils the combined SIRO/CIO function (DGInfo) and the Departmental Security Officer are both accountable to the 2nd PUS, who authorises DGInfo to manage the detailed, day-to-day SIRO business, on his behalf, with the full support of the Defence Board.

Recommendation 30: MOD to define the full scope of responsibilities for the Departmental Chief Information Officer functions.

Recommendation 31: MOD to reinforce the authority of the MOD SIRO to act on behalf of the Defence Operating Board in respect of information risk.

Recommendation 32: MOD and TLBs to consider formalising a network of TLB CIOs and SIROs to provide coherent advice on the exploitation, security and assurance of information as a critical business asset.

ACCREDITATION WITHIN THE MOD

24. Proper accreditation of systems, cited as a 'Mandatory Minimum Measure' by the Cabinet Office, is vital to ensuring the correct handling of personal data within Department. However, there a number of concerns about the current state of accreditation across the Department, which can be summarised as follows:

- a. The current cadre of accreditors within the Department is too small to cope with the scale of the task it faces. DSSO accreditation is currently 15 short of the required manning (of 60). The manning total is itself reckoned to be some 40 short of what would truly be required to accredit all major systems properly.
- b. As a consequence, the Department can only accredit systems currently in development, or those which are the subject of major reviews. The size of the sample of each system which they can take in order to carry out accreditation is also limited to the resources available to them. This constitutes a significant risk to the Department, but there is at present no formal Departmental recognition of this fact.

Recommendation 33: MOD to determine the level of risk it is prepared to bear in the area of accreditation, and resource the accreditors accordingly.

- c. Professionalisation. There is no professional head of accreditation within the Department. For instance the present head of DSSO is being replaced in June by a non-specialist.

Recommendation 34: MOD to appoint a professional head of accreditation with MOD.

- d. Accreditors, in general, are not yet fully attuned to the need to treat aggregated personal data as sensitive information.

Recommendation 35: Accreditors to receive appropriate training to enable them to address data protection issues.

THE OVERALL APPROACH TO THE MANAGEMENT OF PERSONAL DATA

25. Discussions in MOD and with the private sector suggest that the management of personal data is best achieved through three complementary elements:

- a. Forced Compliance. Technical and procedural measures, which force users to adopt proper data management practices in order to physically operate the systems.
- b. Soft Power. Awareness, training and education in personal data management.

c. Hard Power. Censure and punishment for improper data management and losses of personal data.

26. The Soft Power aspects of Awareness, Training and Education are discussed in more detail in paragraphs 37-44. However, the other two elements comprise the following.

27. Forced Compliance. There are a variety of means by which an organisation can ‘force’ users into proper data and information management behaviours, using technology, rules and regulations. These include but are not limited to:

- a. At the most basic level, the use of passwords, both for login and for encryption.
- b. Vetting of staff using the systems, and allocation of appropriate permissions to use them.
- c. Firewall access protocols.
- d. Physical protection of sensitive systems.
- e. Proving awareness of appropriate regulations and data management systems prior to being able to access them. For instance, by having to pass an exam/test, and following appropriate training before one can access the system.

28. The Department already adopts a number of these procedures. For example, the PPPA use access control blocks to prevent staff from inappropriately accessing data. However, the Department could further explore the technological methods of forced compliance and of monitoring abuses/ incorrect practice in using the system. Further contact between MOD and the private sector can be facilitated to enable discussions on this.

Recommendation 36: MOD to consider adopting appropriate technological solutions to achieve compliance with data protection regulations.

29. The concept of making users prove their understanding of their personal data management obligations prior to being able to use the system is a valuable one. The approach is not in evidence in the Department at present. It is understood that DII/F users must read and sign the Sy Ops prior to being able to log on to DII/F, but this does not in itself verify they have understood them.

Recommendation 37: System users to be made to prove, in quantifiable terms, their ability to handle personal data, prior to being given access to the relevant systems.

30. Hard Power: There is anecdotal evidence that the censure and punishment handed out to those who lose, compromise or misuse personal data within the Department is inconsistent at present. Serious compromises of personal data must invoke appropriate punishment, in order to create a deterrent effect and to emphasise the seriousness of such losses.

Recommendation 38: MOD to review and formalise a coherent system of censure and punishment for those who lose or compromise personal data, where the level of punishment reflects the scale and seriousness of the loss; seeking to apply this equitably, regardless of whether the individual responsible is military or civilian, government employee or contractor.

DATA PROTECTION AND SECURITY - KEEPING IT SIMPLE

31. All MOD staff, regardless of rank or role, are likely to have to handle personal data and information at some point. Simplicity is the key to enabling them to understand how to manage it effectively. Stakeholders at all levels agreed that present guidance on information and personal data management does not meet the requirements of MOD staff as a whole. This is because the guidance as it stands is:

a. Too large and unwieldy. JSP 440, the Department's chief document on security, runs to hundreds of pages. System and Security Operating procedures are commonly 90-100 pages. The language used is often specialist and impenetrable to lay readers.

b. Contradictory, and exists in multiple locations. In some instances JSP 440 guidance seems to contradict with individual system security guidance. The confusion over the direction for TAFMIS encryption is also indicative of how multiple documents and guidance notes can confuse the average user.

c. Too slow to catch up with the current environment. Because the documents are often large, it can sometimes take a significant amount of time to update them in light of the fast-moving pace of technology, or a changing threat picture.

32. Security and information management is a complex business, and a place exists for detailed guidance on how precisely to manage this. However, there is a clear desire among Commanders for briefer (maximum 10 page) guidance that gives MOD staff at all levels a clear picture of their obligations with regard to data and information management, and how to meet these.

Recommendation 39: Clear, brief guidance (ideally a 10 page limit) to be produced that is designed with the end user in mind. User feedback to inform future iterations.

Recommendation 40: Authoritative policy documents like JSP 440 to remain; but with 'break-out' documents on e.g. the latest technological developments accompanying them.

33. Another element of simplicity is ensuring that staffs handle and store only the very minimum amount of data required to carry out their job. Had this principle been applied, the RN recruiter on 9 January 2008 would not have been in possession of 600,000 records. The RAF recruiters and DVA vetting officers, for example, currently only carry the immediate records of those individuals they will meet on their daily appointments. In both cases this has led them to conclude that they do not need to carry laptops at all.

34. The default behaviour across the Department, however, continues to be to store and collate as much data as possible, for ease of access, in order to meet Freedom of Information requests from the public, Parliamentary Questions, or media enquiries, or to act as body of data on which to base research and analysis. As noted above, much of this is MOD HQ-driven. However, it has to be recognised that the Department is left with an unnecessarily large store of personal data.

Recommendation 41: MOD to implement the principle of storing and handling only the minimum amount of personal data required to carry out core business.

Recommendation 42: MOD to implement a challenge process, both in terms of deciding whether personal data should be kept in the first place, and then on whether it should be accessed and downloaded on to removable media devices.

DISPOSAL OF DATA DEVICES AND MANAGING UNINTENDED CONSEQUENCES

35. An immediate consequence of the withdrawal of unencrypted laptops and data devices, and the disposal of those whose encryption was either unfeasible or unaffordable, was that some dispossessed users felt obliged to use their private devices to fulfil essential tasks, such as writing annual reviews. These documents represent personal data and are embraced by the Data Protection Act. There is evidence that personal devices are being used for other, classified, work. The perpetuation of this behaviour, which is well-intentioned but misguided, constitutes a significant risk to the Department.

36. The Data Protection Act and Security Regulations effectively preclude the use of private computers and USB data devices for Departmental business. However, technical solutions, such as encrypted USB memory sticks, may offer an affordable, manageable, technical solution.

Recommendation 43: Urgent consideration to be given to procuring a simple, affordable solution to enable the safe, authorised, use of personal (privately owned) computers for limited Government tasks, on an individually licensed basis.

Recommendation 44: Urgent consideration to be given to offering free, safe, disposal of personal data devices.

AWARENESS

37. There is now greater awareness of the personal data security issue within the Department than before 2008. However, the picture is uneven across the Department. This presents risks and vulnerabilities, given the large amounts of personal data held by the Department.

38. Awareness outside MOD HQ is lacking in a number of areas, including the following:

- a. Scope and scale of information risks.
- b. Extent of personal and corporate liabilities under DPA 1998.
- c. Mitigation measures already set out in existing regulations.
- d. Accountabilities for audit and compliance.
- e. Accounting procedures and safe disposal regulations for hard drives and USB data devices.

Recommendation 45: Urgent arrangements to be made to ensure awareness across the Department of risks and mitigation procedures. Consideration to be given to adopting the RN ‘road show’ approach.

39. Ultimately, it is the individual responsibility of data users to ensure that they protect that data appropriately. However, it is the duty of the organisation to ensure that individuals are appropriately informed to enable them to carry out this responsibility. MOD, until recently, did not carry out this function effectively.

40. There is a varied understanding of the threat posed to personal data security and information systems (particularly removable media devices) across the Department. More than one stakeholder pointed out that good security and data management practice often flows directly from a mature appreciation, by users at all levels, of the threat. For instance, during the Cold War, each and every person involved in handling crypto material was aware of the very damaging consequences should it be compromised. There is no evidence that a similar mentality existed as regards personal data (at least not before 9 January 2008).

Recommendation 46: Arrangements to be made for senior leaders and managers to receive a comprehensive briefing on the current threat picture and for formal updates at appropriate intervals.

Recommendation 47: The current threat picture to be clearly and briefly set out to other relevant MOD staff, as a matter of urgency, with formal updates at appropriate intervals.

41. However, much work is in progress within the Department to raise awareness of information security issues. VCDS is developing an action plan, which has tasked the Defence Concepts and Doctrine Centre to produce the conceptual basis on which

Defence should approach security in the electronic age. This encompasses protective and operational security and takes account of the whole range of vulnerabilities, personal and corporate, that bear on the issue. The action plan will also identify and take account of the security vulnerabilities that people in Defence (military and civilian) face in all realms (in their lives and on operations) and what this means in basic security and awareness terms. Another element involves the development of a Training Needs Analysis into all aspects of security training, which will identify the priorities for training effort. The organisation of the Department's security stakeholders is set out at Annex L.

Recommendation 48: Security Doctrine and Operational Security work to be at the heart of the campaign for raising awareness of the importance of information and data to the Department and the significance of protection measures.

42. Increased awareness will stimulate effective leadership, vital to ensuring proper data management within the Department. Leadership by example will have a significant effect. As one stakeholder noted, young officers are today planning and executing operations of greater complexity than ever before. Hence, there is the capability within MOD to understand the issues and to provide the necessary leadership.

TRAINING, EDUCATION AND PROFESSIONALISM

43. To achieve increased awareness, greater training and education is required on personal data handling at all levels of the Department. Current training does exist, but there is a lack of awareness of it among staff and/or a lack of resources and will to undergo the training.

44. There is scope for improving the training and education of data management within the Department, along the lines of the following key principles:

a. The policy must come first. The Department and TLBs must articulate clear requirements for data management, which training organisations can then use to develop courses for users.

Recommendation 49: MOD to review all the current training on Data Protection and Information Management, and identify the uptake by the relevant post-holders, in order to determine future training needs.

b. Timely training. The sooner an individual can be trained in proper data management, the more beneficial for the Department. Stakeholders suggested a key role here for initial training establishments (and in the case of civil servants, induction training). This should then be supported by continued career training and education – for instance, the Defence Academy could have a role in teaching information exploitation and risk management within the context of the operational art, perhaps as part of the Higher Command and Staff Course and Advanced Command and Staff Courses and within the curricula of the Defence Management and Technology College.

c. A Joint Service Approach. Stakeholders disagreed on the extent to which future training and education in this area should be truly Joint. Some were in favour of an overall Joint approach, others felt that distinctions between Single Service interpretations and priorities should be preserved, where these were still relevant. However, it is important for the Defence community, including key commercial partners, to develop a world-class body of knowledge upon which the Department can draw.

Recommendation 50: Full use to be made of the Joint Training and Education institutions, such as the Defence Academy and proposed Defence Security School¹, in providing education and training in the effective exploitation and protection of information and data, including obligations under DPA 1998.

d. Resources will be required. A number of stakeholders made the point that increased training and education would require a commensurate uplift in resources, or a rebalancing of existing resources. For instance, the Defence College of Management and Technology calculated that providing truly comprehensive Senior Information Officer and Manager training would require some 8-10 times the resource currently expended on the short courses for this.

FINANCING AND RESOURCES

45. It is clear that, even though the integration of improved data and information management procedures into MOD daily business should not, in theory, be an onerous task, a significant amount of work may still be required.

46. A number of the recommendations within this report may require additional staff and resources, or a re-balancing of existing assets. These include:

- a. Use of technology to bring about Forced Compliance.
- b. Urgent and regular audit and cleansing of data holdings.
- c. Full audit of MOD PDA, USB and other mobile media holdings.
- d. Increased investment in accreditation.
- e. Concentrated efforts to improve awareness, training and education –this may require additional training courses, additions to existing syllabi, or investment in awareness campaigns.

¹ Deriving benefit from the potential offered by the Defence Security School is conditional on the resources it receives (including the manning of the project team currently taking the requirement forward)

47. It is acknowledged that the resources to meet these recommendations would need to be found within the context of the current challenging Planning Round and ongoing efficiency work, including the Streamlining initiative. However, any decision not to invest in achieving better information data management implies persisting with the high degrees of reputational and operational risk which the Department is currently carrying.

Recommendation 51: Decisions on resourcing this initiative to be taken at Defence Board Level.

CONCLUSIONS

48. The Challenge to MOD. A culture of formal, rigorous Information Risk management and security of personal data has yet to be embedded across the Defence community. The recent losses, though highly regrettable, have at least highlighted this important issue.

49. MOD has, traditionally, placed a high priority on classifying and protecting documents and information that present a security risk to defence capabilities. However, the same degree of rigour and corresponding level of resource has not yet been applied to the protection of information and data held on electronic devices, and infrastructure. This constitutes a significant risk to the Department. The reputational damage of the data loss of 9 January 2008, and other recent similar losses in Government, should change this.

50. It is possible that the Cabinet Office review will recommend that aggregated personal data should be classified as equivalent to Confidential. MOD compliance with the Cabinet Office work, particularly in terms of this revised classification of aggregated personal data, will considerably strengthen its ability to protect and handle personal data properly. However, this is dependent on creating once again within the Department a culture that treats information as a strategic asset, issues clear guidance on how to protect it based on a firm understanding of the threat, and provides strong leadership to manage the associated risks. In particular, the Department will need to find a way of restoring its traditional disciplines in security, yet doing so within the new context of a modern data-rich environment. The recommendations of this report can only be a starting point in this regard.

51. Vulnerability can best be reduced by:

- a. Increasing individual and collective awareness of legal liabilities, risks and mitigation procedures.
- b. Keeping data holdings on any particular systems to the minimum required.
- c. Adopting a disciplined approach to carrying data on mobile devices.
- d. Encrypting data to the maximum feasible extent in order to reduce the likelihood of the data being accessed.
- e. Assuring effective audit and compliance procedures.

52. MOD, as with all organisations which hold and process large amounts of personal data, will always be at risk of future losses, perhaps significant ones. In that context the Department must improve its recording procedures, learn from the experience of recent losses, and do all this with the full knowledge that such incidents cause significant operational and reputational damage.

LIST OF ANNEXES

- A. Summary of Recommendations**
- B. List of MOD Interviewees**
- C. Glossary of Terminology**
- D. Abbreviations and Acronyms**
- E. Data Protection Act 1998 (extract)**
- F. Chronology of TAFMIS Events**
- G. TAFMIS Programme Governance (TAFMIS Sy Ops)**
- H. TAFMIS Programme Governance (ARTD Perspective)**
- I. Extract from DataVault User Instruction**
- J. Defence Information Infrastructure (DII)**
- K. MOD Departmental Structure for Implementation and Compliance with DPA 1998**
- L. The Organisation of the MOD's Security Stakeholders**

ANNEX A –SUMMARY OF RECOMMENDATIONS

1. PROCESSES

Recommendation 1: RN to undertake a review of their recruiter process and, in particular, the need to use mobile devices holding a complete copy of the recruiter database.

Recommendation 3: Supervising officers to be rigorous in enforcement of security instructions.

Recommendation 4: It has not been possible to locate evidence that would support formal disciplinary action. However, it is recommended that the senior leadership in ARTD and in EDS should review the project management processes and procedures, taking appropriate remedial action.

Recommendation 5: MOD to review DPA retention policy to remove potential ambiguities and ensure clarity where variations exist.

Recommendation 6: Where MOD or an MOD contractor provides data management services, there should be an agreement between the relevant parties detailing responsibilities with reference to MOD's DPA record retention policy for personal data types.

Recommendation 7: Contractor to be tasked to cleanse TAFMIS data base as a matter of urgency.

Recommendation 8: MOD to show greater rigour in ensuring that system security procedures are enforced.

Recommendation 10: That all MOD organisations and business units report thefts and losses of removable media in strict accordance with JSP541.

Recommendation 11: MOD to review and adapt established staff procedures and processes, taking account of the opportunities and vulnerabilities implicit in new ICT.

Recommendation 12: MOD to carry out a full audit of its total personal data holdings, based on the work already completed as part of compliance with the Cabinet Office review.

Recommendation 13: MOD to introduce policy and procedures for both data cleansing and data governance, in order to ensure that boards understand the nature and scale of their data holdings and instigate appropriate audit and compliance measures.

Recommendation 14: MOD to carry out a risk-benefit analysis on the requirement to hold large amounts of personal data to meet Centre tasking.

Recommendation 15: That MOD identifies and facilitates the sharing of good practices.

Recommendation 16: A doctrine for Information Exploitation and Protection to be developed in order to set out the principles by which the UK's defence forces will deliver the Information capability underpinning British Defence Doctrine.

Recommendation 17: A coherent, Joint Service and Civil Service, awareness campaign to be launched to highlight the importance of information and data as a key operational and business asset, with appropriate attention devoted to exploitation and protection, within the law.

Recommendation 18: Information Risk to be addressed as a standing risk item on all Executive Boards and Audit Committees.

Recommendation 19: Mandated assurance processes analogous to those for Health and Safety to be introduced for Information Risk.

Recommendation 20: Information Risk to be formally assessed in Capability Reviews and in Office of Government Commerce (OGC) Gateway Reviews.

Recommendation 22: MOD to ensure that the governance processes for legacy programmes, and project approval and acceptance into service, take account both of the legal requirements of the Data Protection Act and of security accreditation.

Recommendation 25: That the Department supports initiatives making personal data accessible through secure links to central servers, on the basis that clear guidelines are in place for onward storage of this data, and the system itself is both secure and has adequate redundancy.

Recommendation 26: MOD to produce clear policy on sharing personal data with third parties, including changes to standard contractual clauses as required.

Recommendation 27: To instigate a full census of non-laptop removable media device holdings, in order to ensure that they are formally approved and accounted for on a routine basis.

Recommendation 28: MOD to implement guidelines on the storage of personal data on these devices, including the requirement for encryption, as necessary.

Recommendation 29: MOD to reiterate, or revise, Departmental guidance on the use of private mobile media devices to process MOD data.

Recommendation 32: MOD and TLBs to consider formalising a network of TLB CIOs and SIROs to provide coherent advice on the exploitation, security and assurance of information as a critical business asset.

Recommendation 33: MOD to determine the level of risk it is prepared to bear in the area of accreditation, and resource the accreditors accordingly.

Recommendation 34: MOD to appoint a professional head of accreditation with MOD.

Recommendation 39: Clear, brief guidance (ideally a 10 page limit) to be produced that is designed with the end user in mind. User feedback to inform future iterations.

Recommendation 40: Authoritative policy documents like JSP 440 to remain; but with 'break-out' documents on e.g. the latest technological developments accompanying them.

Recommendation 45: Urgent arrangements to be made to ensure awareness across the Department of risks and mitigation procedures. Consideration to be given to adopting the RN 'road show' approach.

Recommendation 51: Decisions on resourcing this initiative to be taken at Defence Board Level.

2. **PEOPLE**

Recommendation 2: MOD to ensure that all employees and contractors understand what key information and documents must be maintained as records, and to highlight consequences of failing to do so.

Recommendation 9: MOD to ensure that individual and corporate responsibilities under DPA 1998 are understood and complied with.

Recommendation 23: Detailed accountabilities for Data Protection across the Department to be clearly articulated.

Recommendation 30: MOD to define the full scope of responsibilities for the Departmental Chief Information Officer functions.

Recommendation 31: MOD to reinforce the authority of the MOD SIRO to act on behalf of the Defence Operating Board in respect of information risk.

Recommendation 38: MOD to review and formalise a coherent system of censure and punishment for those who lose or compromise personal data, where the level of punishment reflects the scale and seriousness of the loss; seeking to apply this equitably, regardless of whether the individual responsible is military or civilian, government employee or contractor.

Recommendation 41: MOD to implement the principle of storing and handling only the minimum amount of personal data required to carry out core business.

Recommendation 42: MOD to implement a challenge process, both in terms of deciding whether personal data should be kept in the first place, and then on whether it should be accessed and downloaded on to removable media devices.

Recommendation 46: Arrangements to be made for senior leaders and managers to receive a comprehensive briefing on the current threat picture and for formal updates at appropriate intervals.

Recommendation 47: The current threat picture to be clearly and briefly set out to other relevant MOD staff, as a matter of urgency, with formal updates at appropriate intervals.

Recommendation 48: Security Doctrine and Operational Security work to be at the heart of the campaign for raising awareness of the importance of information and data to the Department and the significance of protection measures.

3. **TRAINING AND EDUCATION**

Recommendation 24: MOD to improve awareness and uptake of current Data Protection Act training.

Recommendation 35: Accreditors to receive appropriate training to enable them to address data protection issues.

Recommendation 37: System users to be made to prove, in quantifiable terms, their ability to handle personal data, prior to being given access to the relevant systems.

Recommendation 49: MOD to review all the current training on Data Protection and Information Management, and identify the uptake by the relevant post-holders, in order to determine future training needs.

Recommendation 50: Full use to be made of the Joint Training and Education institutions, such as the Defence Academy and proposed Defence Security School¹, in providing education and training in the effective exploitation and protection of information and data, including obligations under DPA 1998.

4. **TECHNOLOGY**

Recommendation 36: MOD to consider adopting appropriate technological solutions to achieve compliance with data protection regulations.

Recommendation 43: Urgent consideration to be given to procuring a simple, affordable solution to enable the safe, authorised, use of personal (privately owned) computers for limited Government tasks, on an individually licensed basis.

Recommendation 44: Urgent consideration to be given to offering free, safe, disposal of personal data devices.

¹ Deriving benefit from the potential offered by the Defence Security School is conditional on the resources it receives (including the manning of the project team currently taking the requirement forward)

5. **OTHER**

Recommendation 21: MOD to seek guidance from the Information Commissioner on the status of the TAFMIS database(s) as regards the Data Protection Act.

ANNEX B – LIST OF MOD INTERVIEWEES

| | |
|--------------------------------|--|
| PUS | - Sir William Jeffrey |
| CDS | - Air Chief Marshal Sir Jock Stirrup |
| VCDS | - Gen Sir Timothy Granville-Chapman |
| 2 nd PUS | - Sir Ian Andrews |
| CNS | - Admiral Sir Jonathon Band |
| CGS | - General Sir Richard Dannatt |
| CAS | - Air Chief Marshal Sir Glenn Torpy |
| CINC FLEET | - Admiral Sir Mark Stanhope |
| CINC LAND | - General Sir David Richards |
| CINC AIR | - Air Chief Marshal Sir Clive Loader |
| CDM | - General Sir Kevin O’Donoghue |
| NED | - Mr Ian Rushby |
| 2SL | - Vice Admiral Sir Adrian Johns |
| AG | - Lieutenant General Sir Freddie Viggers |
| DCDS(C) | XXXXX |
| DCDS(EC) | XXXXX |
| DCDS(H) | XXXXX |
| Director Defence Academy | XXXXX |
| DE&S CCM | XXXXX |
| Personnel Director | XXXXX |
| S&T Director | XXXXX |
| MDP DCC/COS | XXXXX |
| DCINC FLEET | XXXXX |
| FOSNNI | XXXXX |
| Comdt JSCSC | XXXXX |
| CE SPVA | XXXXX |
| COS LAND | XXXXX |
| DG ATR | XXXXX |
| DG DCDC | XXXXX |
| DG T&E | XXXXX |
| AOC 22 Gp (Trg) | XXXXX |
| PJHQ DCJO Op Sp | XXXXX |
| FLEET Cmd Sec | XXXXX |
| DG Sec Land Forces | XXXXX |
| DGCP | XXXXX |
| DGS&S | XXXXX |
| DE&S COS | XXXXX |
| DG Info | XXXXX |
| CE PPPA | XXXXX |
| Comdt DCMT | XXXXX |
| Principal Cranfield University | XXXXX |
| LAND CIO | XXXXX |
| D CBM | XXXXX |
| DTIO | XXXXX |
| AIR ACOS A6 | XXXXX |
| DGMO | XXXXX |
| DII IPTL | XXXXX |
| D Info Exp | XXXXX |

| | |
|---------------------------|--------|
| Hd ARAG | XXXXXX |
| D Def Sy | XXXXXX |
| Hd DSSO | XXXXXX |
| Hd of dbLearning | XXXXXX |
| Hd JSyCC | XXXXXX |
| SPVA DMS | XXXXXX |
| DVA Hd Ops | XXXXXX |
| FLEET Sy Lead | XXXXXX |
| ATRD Hd MIS | XXXXXX |
| ATRD MIS SO2 Sy | XXXXXX |
| ATRD TAFMIS Accreditation | XXXXXX |
| DSSO Accreditation | XXXXXX |
| London AFCO (Bloomsbury) | |
| FLEET Recruiters | |

ANNEX C – GLOSSARY OF TERMINOLOGY

Accreditation - Mandatory MOD requirement for all IT-based systems that electronically store, process or forward official information. It is the process through which it is confirmed that the use of these systems does not pose an unacceptable risk to National security.

Asset - Anything that has value to the organisation, its business operations and its continuity

Authentication - Ensuring that the identity of a subject or resource is the one claimed

Availability - The property of being accessible and usable upon demand by an authorised entity

Business Impact - The result of an information security incident on business functions and the effect that a business interruption might have upon them

Confidentiality - The property that information is not made available or disclosed to unauthorised individuals, entities, or processes

Data Controller - Means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

Impact - The result of an information security incident, caused by a threat, which affects assets

Information Assurance - The confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users

Information Security - Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

Information Security Management System (ISMS) - That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

Integrity - The property of safeguarding the accuracy and completeness of assets

Mitigation - Limitation of the negative consequence of a particular event

Non-repudiation - The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

Personal Data - means data which relate to a living individual who can be identified—

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

Residual Risk - Risk remaining after treatment

Risk - The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the Organization

Risk Acceptance - Decision to accept a risk

Risk Appetite - Attitude taken by an organisation, which in relation to risk minimises the negative and maximises the positive business consequences and their respective probabilities

Risk Analysis - Systematic use of information to identify sources and to estimate the risk

Risk Assessment - The overall process of risk analysis and risk evaluation

Risk Avoidance - Decision not to be involved in, or action to withdraw from, a risk situation

Risk Evaluation - Process of comparing the estimated risk against given risk criteria to determine the significance of risk

Risk Identification - Process to find, list and characterise elements of risk

Risk Management - Process of coordinating activities to direct and control an organisation with regard to risk

Risk Management System - Set of elements of an organisation's management system concerned with managing risk

Risk Reduction - Action taken to lessen the probability, negative consequences, or both, associated with risk

Risk Retention - Acceptance of the burden of loss, or benefit of gain, from a particular risk

Risk Transfer - Sharing with another party the burden of loss or benefit of gain, for a risk

Risk Treatment - The process of selection and implementation of measures to modify risk

Statement of Applicability - Document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes

Threat - A potential cause of an incident that may result in harm to a system or organization

Vulnerability - A weakness of an asset or group of assets that can be exploited by one or more threats

ANNEX D – ABBREVIATIONS AND ACRONYMS

| | | |
|--------|---|---|
| ACSC | - | Advanced Command and Staff Course |
| AFPAA | - | Armed Forces Pay & Administration Agency |
| AFCO | - | Armed Forces Careers Office |
| AG | - | Adjutant General |
| ARTD | - | Army Recruiting & Training Division |
| ATRA | - | Army Training & Recruiting Agency |
| CESG | - | Communications Electronics Security Group |
| CIO | - | Chief Information Officer |
| CMN | - | Change Management Note |
| DASA | - | Defence Analytical Services Agency |
| DG | - | Director General |
| DDefSy | - | Directorate of Defence Security |
| DII/F | - | Defence Information Infrastructure Future |
| DIN | - | Defence Instruction Notice |
| DSSO | - | Defence Security Standards Organisation |
| DPA | - | Data Protection Act |
| DPO | - | Data Protection Officer |
| DVA | - | Defence Vetting Agency |
| EDS | - | Electronic Data Systems |
| GCHQ | - | Government Communications Headquarters |
| HCSC | - | Higher Command and Staff Course |
| HRMS | - | Human Resources Management System |
| ICT | - | Information Communications Technology |
| JSP | - | Joint Service Publication |
| JSyCC | - | Joint Security Co-ordination Centre |
| MOD | - | Ministry of Defence |
| OGC | - | Office of the Government Commerce |
| PDA | - | Personal Data Assistant |
| PJHQ | - | Permanent Joint Headquarters |
| PUS | - | Permanent Under Secretary |
| RAF | - | Royal Air Force |
| RN | - | Royal Navy |
| SofS | - | Secretary of State |

| | |
|-------------|--|
| SIRO | - Senior Information Risk Owner |
| SOPs | - Standard Operating Procedures |
| SPVA | - Service Personnel & Veterans Agency |
| Sy Ops | - Security Operating Procedures |
| TAFMIS | - Training Administration and Financial Management Information System |
| TAFMIS-T | - Training |
| TAFMIS-C | - Classroom |
| TAFMIS-R | - Recruiting |
| TAFMIS-R(H) | - Recruiting (Harmonised) |
| TLB | - Top Level Budget |
| USB | - Universal Serial Bus |
| VCDS | - Vice Chief of Defence Staff |

ANNEX E – EXTRACT FROM DATA PROTECTION ACT 1998

THE DATA PROTECTION PRINCIPLES

PART I THE PRINCIPLES

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

- (a) at least one of the conditions in Schedule 2 is met, and
- (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

PART II INTERPRETATION OF THE PRINCIPLES IN PART I

The first principle

1 (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

(2) Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who—

- (a) is authorised by or under any enactment to supply it, or
- (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom.

2 (1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless—

(a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and

(b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).

(2) In sub-paragraph (1)(b) “the relevant time” means—

(a) the time when the data controller first processes the data, or

(b) in a case where at that time disclosure to a third party within a reasonable period is envisaged—

(i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,

(ii) if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or

(iii) in any other case, the end of that period.

(3) The information referred to in sub-paragraph (1) is as follows, namely—

(a) the identity of the data controller,

(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,

© the purpose or purposes for which the data are intended to be processed, and

(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

3 (1) Paragraph 2(1)(b) does not apply where either of the primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the Secretary of State by order, are met.

(2) The primary conditions referred to in sub-paragraph (1) are—

(a) that the provision of that information would involve a disproportionate effort, or

(b) that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 (1) Personal data which contain a general identifier falling within a description prescribed by the Secretary of State by order are not to be treated as processed fairly and lawfully unless they are processed in compliance with any conditions so prescribed in relation to general identifiers of that description.

(2) In sub-paragraph (1) “a general identifier” means any identifier (such as, for example, a number or code used for identification purposes) which—

(a) relates to an individual, and

(b) forms part of a set of similar identifiers which is of general application.

The second principle

5 The purpose or purposes for which personal data are obtained may in particular be specified—

(a) in a notice given for the purposes of paragraph 2 by the data controller to the data subject, or

(b) in a notification given to the Commissioner under Part III of this Act.

6 In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

The fourth principle

7 The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where—

(a) having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data, and

(b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact.

The sixth principle

8 A person is to be regarded as contravening the sixth principle if, but only if—

(a) he contravenes section 7 by failing to supply information in accordance with that section,

(b) he contravenes section 10 by failing to comply with a notice given under subsection (1) of that section to the extent that the notice is justified or by failing to give a notice under subsection (3) of that section,

(c) he contravenes section 11 by failing to comply with a notice given under subsection (1) of that section, or

(d) he contravenes section 12 by failing to comply with a notice given under subsection (1) or (2)(b) of that section or by failing to give a notification under subsection (2)(a) of that section or a notice under subsection (3) of that section.

The seventh principle

9 Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected.

10 The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

11 Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—

- (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
- (b) take reasonable steps to ensure compliance with those measures.

12 Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless—

- (a) the processing is carried out under a contract—
 - (i) which is made or evidenced in writing, and
 - (ii) under which the data processor is to act only on instructions from the data controller, and
- (b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

The eighth principle

13 An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to—

- (a) the nature of the personal data,
- (b) the country or territory of origin of the information contained in the data,
- (c) the country or territory of final destination of that information,
- (d) the purposes for which and period during which the data are intended to be processed,
- (e) the law in force in the country or territory in question,
- (f) the international obligations of that country or territory,
- (g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and
- (h) any security measures taken in respect of the data in that country or territory.

14 The eighth principle does not apply to a transfer falling within any paragraph of Schedule 4, except in such circumstances and to such extent as the Secretary of State may by order provide.

15 (1) Where—

- (a) in any proceedings under this Act any question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any personal data to a country or territory outside the European Economic Area, and
- (b) a Community finding has been made in relation to transfers of the kind in question, that question is to be determined in accordance with that finding.

(2) In sub-paragraph (1) “Community finding” means a finding of the European Commission, under the procedure provided for in Article 31(2) of the Data Protection Directive, that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Article 25(2)

ANNEX F – CHRONOLOGY OF TAFMIS EVENTS

Events pre-January 2008

| Serial | Date | Event | MOD | EDS | Document ref | Comments |
|--------|--------------|--|----------------|-------|--|---|
| A01 | Oct 1996 | TAFMIS Development and Service Provision Agreement inc. Schedule 18 Security Model | CCTA | | PRT 141/496 S18v14I | |
| A02 | Sep 1997 | TAFMIS in service date plus contract extension to Aug 2007 | ARTD Hd MIS | | ARTD Brief to Sir E Burton 27 Feb 08 | |
| A03 | Jan 1999 | Recruiting Extension, TAFMIS-R | ARTD Hd MIS | | ARTD Brief to Sir E Burton 27 Feb 08 | |
| A04 | Jan 2002 | RN and RAF Recruiting Extension, TAFMIS-R(H) | ARTD Hd MIS | | ARTD Brief to Sir E Burton 27 Feb 08 | Developed as separate contract with AFPAA |
| A05 | Nov/Dec 2001 | DataVault encryption added to laptops used in Northern Ireland | | XXXXX | EDS Note to Burton Review | |
| A06 | Jan 2003 | Requirement to add encryption to all laptops. New laptops from 1 Apr 03, existing laptops by 1 Jan 06. | DDefSy | | DCI 23/03 JSP440 Issue 3.0 | |
| A07 | Jan 2003 | EDS notified of changes for cryptographic protection for all laptops and ATRA policy to use DataVault. | DGAT R | | D/ATRA/2203/MIS | |
| A08 | Feb 2003 | JSP 440 advises all new laptops are to have approved encryption and existing laptops by Jan 06 | DDefSy | | JSP 440 Issue 3.0 | |
| A09 | Mar 2003 | EDS advise that Data Vault encryption could be installed before Apr 06. | ARTD | | Security of TAFMIS Laptops Chronology Narrative | |

| | | | | | | |
|-----|----------|--|--------------|--------|---|--|
| A10 | Apr 2004 | AGIS SO2 Info Man Sy confirmed that ATRA could issue new laptops to users unencrypted providing DataVault was installed before Jan 06. | ARTD | | Security of TAFMIS Laptops Chronology Narrative | |
| A11 | Jun 2004 | Contract Management Note 2548, formal instruction to EDS to install suitable encryption mechanism. | ARTD | | Security of TAFMIS Laptops Chronology Narrative | |
| A12 | Aug 2004 | TAFMIS-R(H) laptop taken from vehicle in Bristol belonging to AFCO Manchester | MOD JSyCC | | | |
| A13 | Jul 2005 | EDS submit to ATRA Data Vault technical solution | ARTD | | Security of TAFMIS Laptops Chronology Narrative | |
| A14 | Sep 2005 | Monthly CMN review meeting EDS report that Data Vault solution has been approved by Defence Security | ARTD | | Security of TAFMIS Laptops Chronology Narrative | |
| A15 | Dec 2005 | Confidence testing highlights synchronisation defects between DataVault and SQL database on TAFMIS R(H) laptops, application fix required. | | XXXXXX | EDS Note to Burton Review | |
| A16 | Dec 2005 | Theft of two TAFMIS-R Army laptops from AFCO Edinburgh | MOD JSyCC | | | |
| A17 | Feb 2006 | ARTD MIS on behalf of HQ ATRA complete review of DPA Policy | ARTD | | Security of TAFMIS Laptops Chronology Narrative | |

| | | | | | | |
|-----|----------|--|--------------|--------|---|--|
| A18 | Mar 2006 | EDS report that user handout detailing how to operate Data Vault will be distributed to users via email at time of install. | ARTD | | Security of TAFMIS Laptops Chronology Narrative | |
| A19 | Apr 2006 | JSP440 deadline for laptop encryption extended to Jan 2009 for laptops purchased before Apr 2003. (TAFMIS laptops purchased pre Apr 03 need to be encrypted by Jan 09, purchased Apr 03 to Jan 06 encrypted by Jan 09, purchased after Apr 06 encrypted immediately.) | DDefSy | | JSP440 Issue 3.5 | |
| A20 | Apr 2006 | EDS begin testing of TAFMIS-R(H) laptops in preparation for roll-out, testing continues until Jun 06 | ARTD | | Security of TAFMIS Laptops Chronology Narrative | |
| A21 | May 2006 | DataVault installed on 96% of TAFMIS-T and TAFMIS-R laptops. TAFMIS-R(H) laptops still in test and development. | | XXXXXX | EDS Note to Burton Review | |
| A22 | Jun 2006 | ATRA loses agency status following Defence Training Review and is renamed to ARTD | ARTD MIS | | Security of TAFMIS Laptops Chronology Narrative | |
| A23 | Jun 2006 | ARTD MIS request DataVault action closed at Service Delivery Meeting and moved by agreement to Small CMN meeting | | | EDS response to Burton meeting 25/3/08 | |
| A24 | Jul 2006 | TAFMIS-R(H) RAF laptop belonging to Leeds AFCC stolen from car. | MOD JSyCC | | | |

| | | | | | | |
|-----|----------|---|-----------|--|---|--|
| A25 | Aug 2006 | CMN meeting reports Data Vault rollout complete except for 55 TAFMIS-R(H) laptops. Reporting of DataVault then ceases without explanation. | | | Security of TAFMIS Laptops Chronology Narrative | |
| A26 | Sep 2006 | DIN 2006DIN08-020 clarifies MOD laptop encryption deadline detailed in JSP440 Issue 3.5 and requires approval from Principal Security Officer if devices are being replaced/refreshed by DII programme. | DDefSy | | 2006DIN08-020 | No approval sought by ARTD as they believed TAFMIS laptops were compliant. |
| A27 | Oct 2006 | TAFMIS-R(H) laptop taken from car in Manchester. | MOD JSyCC | | | |
| A28 | Apr 2007 | AFPAA transfer responsibility for TAFMIS-R(H) to ARTD. | ARTD MIS | | Security of TAFMIS Laptops Chronology Narrative | |
| A29 | Jul 2007 | JSP 440 Issue 3.6 published and drops requirement to seek approval from Principal Security Officer | | | | |
| A30 | Nov 2007 | ARTD review DPA Policy | ARTD MIS | | Security of TAFMIS Laptops Chronology Narrative | |
| A31 | Nov 2007 | TAFMIS-R(H) user raises Helpdesk call requesting ability to store TRHA local database in DataVault. User requested to raise an RFC, no RFC was raised and call closed Nov 07. | ARTD MIS | | Security of TAFMIS Laptops Chronology Narrative | |

Events post- January 2008

| Serial | Date | Event | MOD | EDS | Document ref | Comments |
|--------|-----------|--|---------------------|-----|---|----------------|
| B01 | 9 Jan 08 | TAFMIS-R(H) RN laptop stolen from locked car boot in Edgbaston, Birmingham | | | | |
| B02 | 10 Jan 08 | Theft of laptop reported to local police and TAFMIS Helpdesk | RN Officer | | D/FLEET/585/1 & Security of TAFMIS Laptops Chronology Narrative | |
| B03 | 11 Jan 08 | Incident reported to Ministers | | | | |
| B04 | 14 Jan 08 | Ministers informed that data was not encrypted | | | | |
| B05 | 16 Jan 08 | 2 nd PUS brief Min(AF) on laptop loss and personal data | 2 nd PUS | | D/VCDS&2ndPUS/2/2/1 | |
| B06 | 15 Jan 08 | Director General Information notified of theft | | | | JSyCC timeline |
| B07 | 16 Jan 08 | TAFMIS laptop recall initiated | | | | JSyCC timeline |
| B08 | 17 Jan 08 | RAF confirm all TAFMIS laptops are secure | | | | JSyCC timeline |
| B09 | 17 Jan 08 | FLEET confirm all TAFMIS laptops are secure | | | | JSyCC timeline |
| B10 | 17 Jan 08 | AFCO Edinburgh verbal report of 2 further TAFMIS-R(H) laptops stolen 21/22 Dec 05 | | | | JSyCC timeline |
| B11 | 18 Jan 08 | LAND confirm all TAFMIS laptops are secure | | | | JSyCC timeline |
| B12 | 18 Jan 08 | AFCO Edinburgh report into laptop thefts | | | | JSyCC timeline |
| B13 | 19 Jan 08 | 2 nd PUS brief Secretary of State on laptop loss and personal data | 2 nd PUS | | D/VCDS&2ndPUS/2/2/1 | |
| B14 | 21 Jan 08 | Secretary of State oral statement to Parliament about the lost of MOD recruitment data, laptops and investigation to be undertaken by Sir Edmund Burton. | SofS | | | |
| B15 | 22 Jan 08 | New rules announced on accreditation of | 2 nd PUS | | D/VCDS&2ndPUS/ | |

| | | | | | | |
|-----|-----------|--|-------------|--------------------|---|----------------|
| | | information systems, encryption of laptops and handling of unencrypted removable IT assets | | | 2/2/1 | |
| B16 | 22 Jan 08 | Bristol AFCO report TAFMIS-R(H) laptop stolen Jul 06 | | | | JSyCC timeline |
| B17 | 25 Jan 08 | Email informing that DataVault encryption product was not deployed on TAFMIS laptops | | | | JSyCC timeline |
| B18 | 28 Jan 08 | EDS confirm no data entries pre date 1997 | ARTD Hd MIS | EDS Acc Exec | Email: ' Update to Candidates pre 1997' | |
| B19 | Feb 08 | DIN announced changes to accreditation and laptop encryption policy | DDefSy | | 2008DIN02-002 | |
| B20 | 1 Feb 08 | EDS admits that their report detailing earliest record date is not 1997 but 1977. | ARTD Hd MIS | EDS Acc Exec | Email: ' Update to Candidates pre 1997' | |
| B21 | 4 Feb 08 | DSSO accreditation review of TAFMIS, draft report | DSSO DDAcc | | DSSO/01-03-05 | |
| B22 | 4 Feb 08 | Burton Review Team assembled in MOD | | | | |
| B23 | 8 Feb 08 | EDS letter to 2ndPUS providing clarification regarding data contained on stolen MoD Laptop | | EDS Vice President | | |
| B24 | 11 Feb 08 | Update on TAFMIS laptop records to APS/SofS | DG Info | | DG Info/9/4/7 (12/08) | |
| B25 | 11 Feb 08 | Sir Edmund Burton notifies key stakeholders of his review process | DG Info | | DGInfo/9/4/7 | |

ANNEX G – TAFMIS PROGRAMME GOVERNANCE (TAFMIS (Sy Ops))

1. ADMINISTRATION

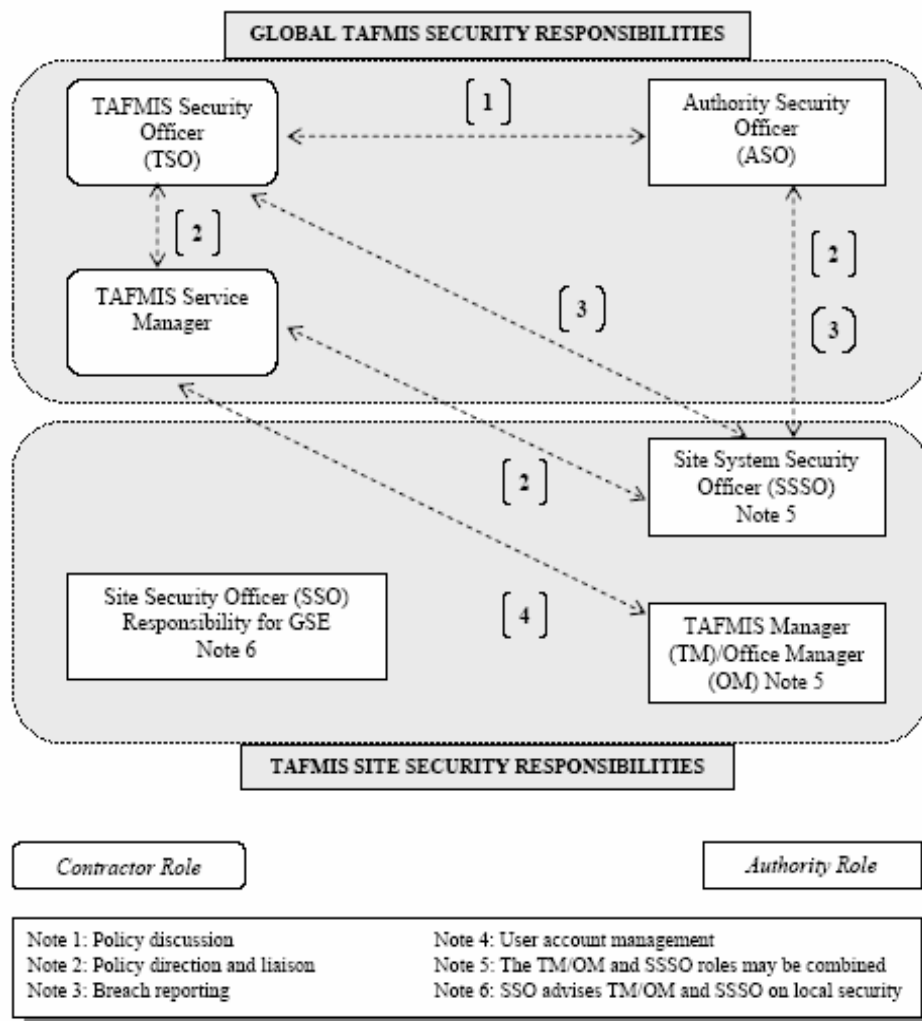
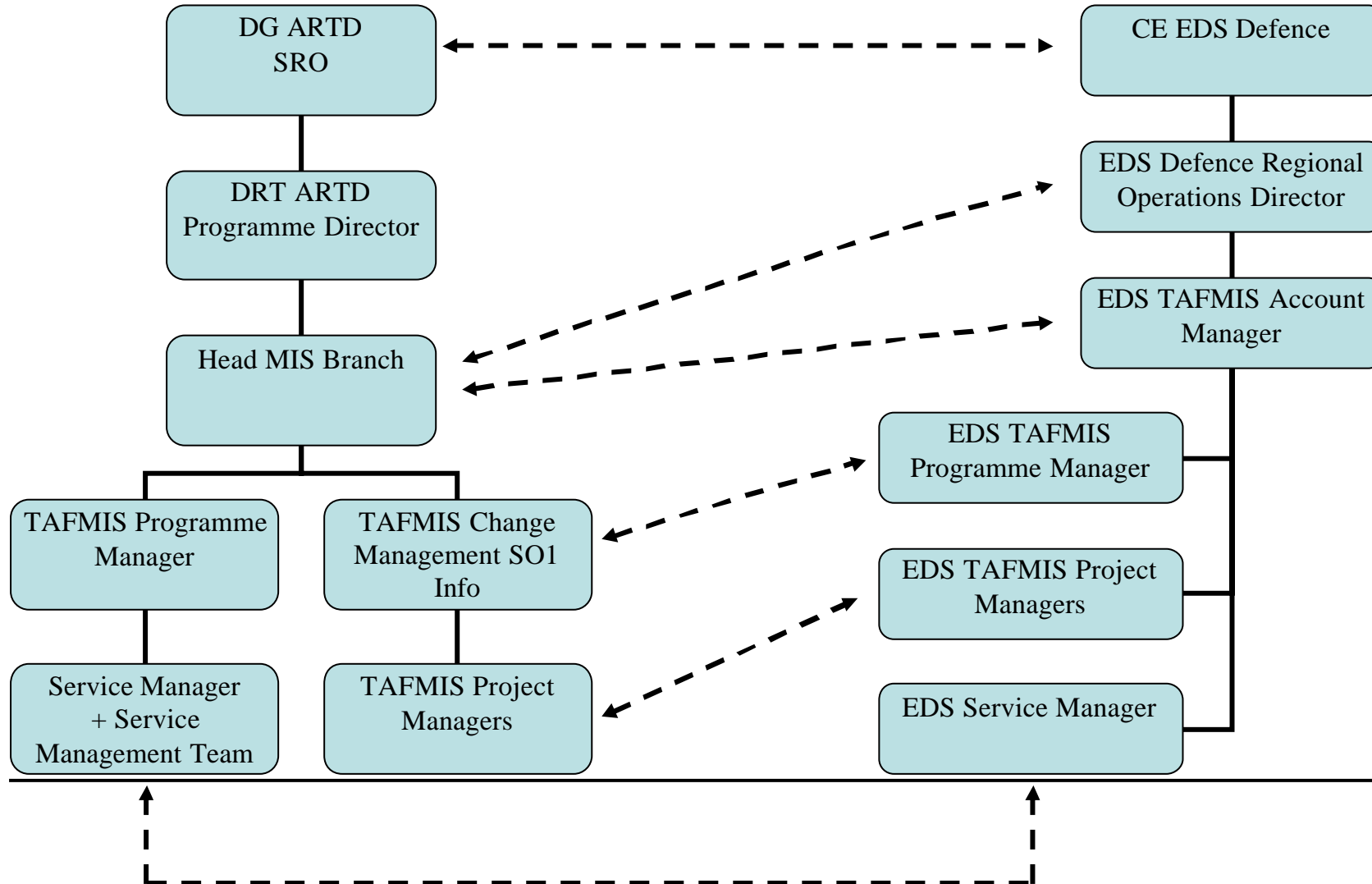


Figure 1: TAFMIS Security Roles and Main Intercommunication Functions

ANNEX H – TAFMIS PROGRAMME GOVERNANCE (ATRD PERSPECTIVE)



ANNEX I – EXTRACT FROM DATAVAULT USER INSTRUCTION

Reflex Data Vault Laptop Encryption User Guide.

EXAMPLE:

Laptop Name: HOKPC6001

Laptop Owner: Daren Oldring

Site: HOOK

Phone Number: 01256 742197

Mobile Phone Number: 07790 491373

Date of proposed installation: March 27th 2006

IMPORTANT for the Attention of **(The Vault Owner)**,

Over the next few weeks we will be remotely installing Reflex Data Vault, a hard disk encryption solution to all laptops within TAFMIS using either SMS or VNC. Reflex Data Vault will create a secure encrypted drive on the user's laptop that will be used for storing all information at **RESTRICTED** level and above. After installation has completed you will notice a new drive within 'My Computer' and 'Windows Explorer' G:.

Installation

The TAFMIS Installation Team will setup an SMS package to be sent to a set number of laptops per day.

You will be contacted on the telephone number(s) you have provided in the datavault pre-installation form that was sent to you to be given your installation date and an AM or a PM slot.

The engineer will then take control of your laptop for a period of 30-40 minutes before releasing it back to you with your passwords for the vault.

NB: if you are a named user then you will need to get the passwords from the laptop owner at your site to be able to unlock the vault.

ANNEX J - DEFENCE INFORMATION INFRASTRUCTURE (DII(F))

WHAT IS DII?

The 1998 Strategic Defence Review (SDR) provided a radical analysis of the UK's security priorities, missions and tasks. As part of this forward-looking strategy the White Paper allocated a high priority to Information Technology and its application in Defence. It was recognised that the infrastructure of the MoD's Information Technology was unable to deliver the required functionality into the Twenty-first century. Hence, the simple vision for transforming defence effectiveness emerged:

- *Vision One Information Infrastructure*. This resulted in the formation of an Integrated Project Team as the MoD lead for creating and managing a Defence Information Infrastructure. The DII IPT mission was quickly established:

MISSION

To deliver to Defence a secure and coherent Information Infrastructure at minimum whole life cost whilst maintaining continuity of service.

What are the DII objectives?

The DII(F) infrastructure will:

- Enable a Defence user to access their IS services at any location both within Defence and remotely.
- Enable two or more users to exchange information, comprehend and manipulate it.
- Enable any user to access any application functionality they require.
- Provide every user of DII with a Quality of Service appropriate to their operational or business requirements.

Why do we need DII?

The 1998 Strategic Defence Review (SDR) provided a radical analysis of the UK's security priorities, missions and tasks. As part of this forward-looking strategy the White Paper allocated a high priority to Information Technology and its application in Defence. Information Technology is seen as the gateway to high capability, integrated forces, and better value for money in Defence. The SDR envisages a "single battle-space in which land, maritime, and air forces will be directed, targeted and supplemented by a new generation of intelligence, surveillance, information and communication systems".

The Defence Information Strategy also identified a need for improved efficiency, effectiveness and communications: Enhanced operational effectiveness - better IT and communication systems will enable greater strategic and operational agility during times of crisis; and greater economy of effort. Therefore, in order to carry out its business, Defence must bring together its information, personnel and equipment into a coherent strategy and set of managed mission and business processes. The success of Defence, and in particular the military operations it performs, is dependent on making information available to the people and processes that need it.

What are the benefits of DII?

By providing the necessary infrastructure, DII will act as a platform for delivering and enabling numerous benefits across the Department.

DII will deliver a range of significant benefits both to end users and the Department as a whole. Some of these will be quantifiable (e.g. IT cost effectiveness, system performance & availability), and others will facilitate improved ways of working (e.g. more effective exchange and sharing of information etc).

Perhaps most importantly, DII provides the bedrock which will enable the Department to meet a number of technology-enabled strategic goals (e.g. Network Enabled Capability (NEC), Joint Operational Picture (JOP), and Information Utilisation (IX)). There will be significant improvements in overall IT cost-effectiveness directly enabled by implementing DII. (e.g. the rationalisation of current applications and cost benefits from centrally managed and supported solutions). These improvements will support the Department in meeting a number of Government-wide initiatives (e.g. Efficiency Review and Freedom of Information).

From an end-user perspective, there will be one common infrastructure – tailored appropriately – enabling significant operational efficiency improvements (e.g. roll-out of uniform world class applications [email/browser/MsOffice] provision). Many additional benefits may be realised by other Defence Change Programme projects (e.g. JAMES (Whole Fleet Management) and Joint Personnel Administration (JPA)), which are reliant on DII.

As further projects in the Defence Change Programme are defined, additional DII benefits will emerge. The DII solution is being built to allow it to take advantage of future technology improvements. A joint DII/ATLAS benefits working team is already mobilised and significant advances have been made on identifying potential benefits and tracking improvements, including an 'early results' programme.

**ANNEX K - MOD DEPARTMENTAL STRUCTURE FOR
IMPLEMENTATION AND COMPLIANCE WITH DPA 1998**

K1: TERMS OF REFERENCE FOR TLB AND AGENCY DATA PROTECTION OFFICERS

The main duties of a Data Protection Officer (DPO) are as follows:

1. You are responsible for promoting Data Protection policy within your area of responsibility. You are to ensure compliance with the Data Protection Act 1998, including the Data Protection Principles and other central guidance.
2. Identify and record the location of the main holdings of personal data in the TLB/ Agency/ Unit, which may include spreadsheets and data bases holding a variety of personal information, so that personal data can be located.
3. Identify and record the purpose for which personal data are being processed and conduct regular checks to ensure that personal data is safeguarded appropriately and is held for legitimate business reasons.
4. Ensure that the privacy and security of all personal data is adequately maintained. Conduct regular audit checks to ensure that personal data is being properly processed in accordance with established Departmental policy and the Information Commissioner's guidelines on audit.
5. Ensure that the conditions for processing personal data are satisfied, with special regard for sensitive personal data processing requirements.
6. Put in place and/or review regularly arrangements to meet Subject Access Requests (SARs) to ensure the specified timeframe is met (i.e. 40 calendar days from receipt of the properly identified SAR to the composite MOD return to the individual) in accordance with the Department's handling policy.
7. Seek and provide advice in liaison with FOIA/ EIRs Focal Points, single Service and civilian DPOs (including the PPPA) with overall responsibility for DPA98, other TLB/Agency DPOs newly (including the newly created APIS PPPA Cell) regarding the disclosure of personal information. The disclosure of information will require consideration under DPA, FOIA, EIR and other legislation, e.g. courts records, other investigations and proceedings, legal advice and in respect of deceased persons.
8. Put in place and /or review the arrangements to manage the correction of entries and the routine deletion of personal information, in accordance with existing Departmental policy on retention periods for the holding of personal data, local and other procedures (e.g. JSPs, Data Protection Guidance Notes).
9. Take appropriate action to maintain awareness within TLB/ Agency of Data Protection issues.

10. The Department has a legal requirement to ensure Data Protection issues are addressed correctly and that personal data is provided with the proper protection it requires as defined under the Act. To ensure adequate resources are made available to this task, the duties of the Data Protection Officer in each unit should be included in the duties of the post and recorded in the individual's Annual Confidential Staff Report/ Performance Assessment and Development Report.

Revised by DG Info-Access Pol – March 2008

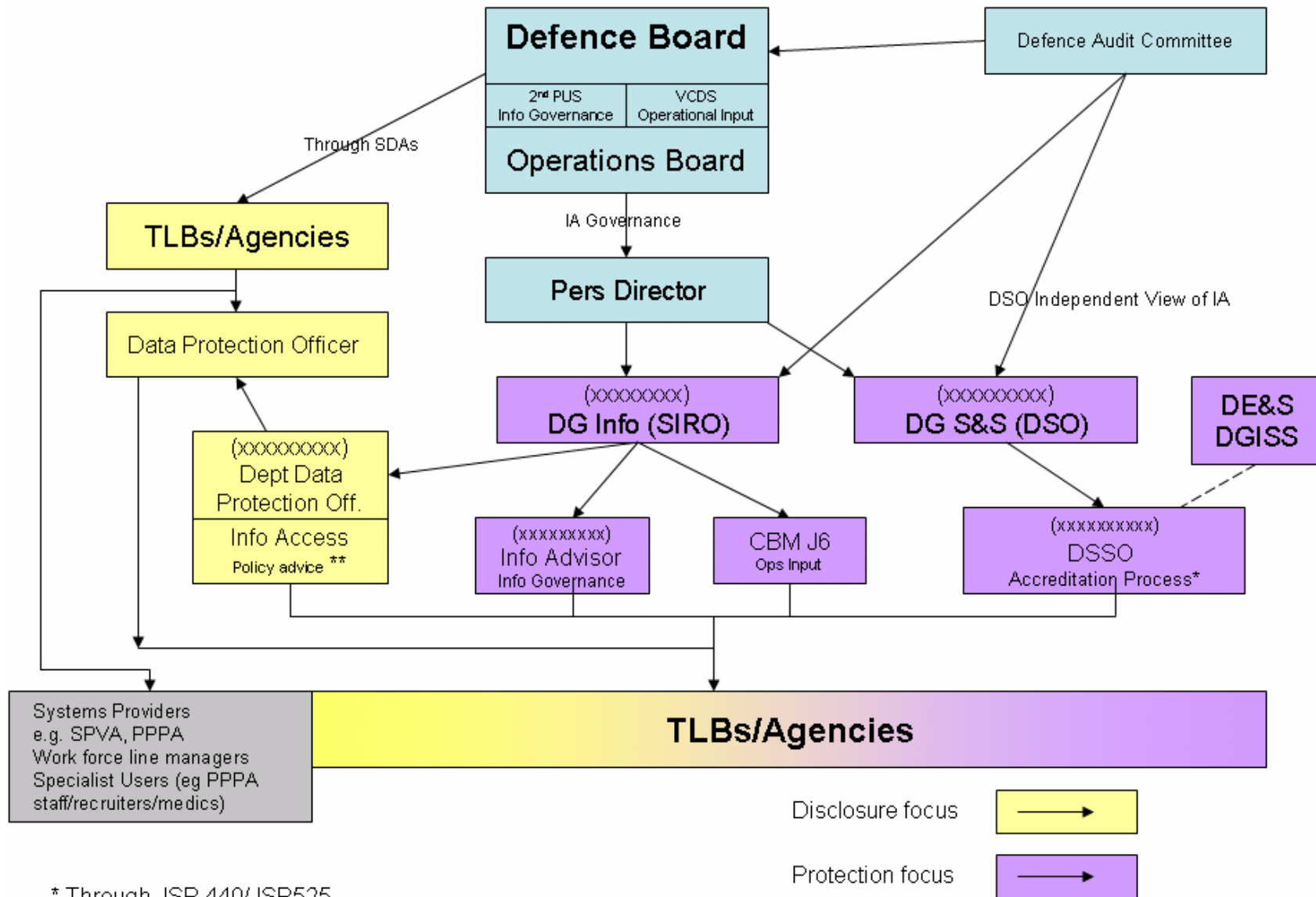
**K2: EXTRACT FROM MOD SERVICE DELIVERY AGREEMENTS –
DIRECTION FROM PUS TO TOP-LEVEL BUDGET HOLDERS
REGARDING DATA PROTECTION OBLIGATIONS**

DPA

You are to ensure that you are able to comply with the MOD's policy for implementing its legal obligations, including those in the [Data Protection Act 1998](#) (DPA 98) and the recommendations of the Hannigan review of the handling of personal data in Government. To this end you will undertake the following actions:

- Appoint a Data Protection Officer (DPO), or Officers, at a level not less than B2 or Service equivalent for your area or each major business unit within it. This individual who should ensure that all systems and processes used for processing, including the obtaining, recording, holding or use or disclosure of such information within your TLB, of information relating to individuals (both Service and civilian) are compliant with the [Data Protection Act 1998](#) and Departmental guidance, including [JSP 400](#).- Disclosure of Information. To this end the DPO will engage with all key stakeholders in your organisation, including information managers, IT and HR/personnel functions and any others.
- Maintain a record of all IT systems used to store personal data and keep this up to date and provide returns to DG Info staff as required.
- Ensure all IT systems are appropriately protected, including encryption.
- Ensure a plan is in place to ensure that all staff in your area complete mandatory training in Data Protection and the handling of personal data appropriate to their post and the data they handle.
- Recording and report any breaches of the Data Protection Act 1998, including the loss of any personal data. Such losses must be reported promptly to DG Info staff.
- Examine periodically your existing record holdings to ensure that you do not hold personal data for longer than is required, and that any personal data held is justified by a continuing business need.

Data Protection Act Policy and Info Assurance Road Map April 2008



* Through JSP 440/JSP525
 ** Through JSP 400

ANNEX L - THE ORGANISATION OF THE MOD'S SECURITY STAKEHOLDERS

