The National Archives

Information Management Assessment

The Ministry of Defence

June 2012

About Information Management Assessments

The Information Management Assessment (IMA) programme is the best-practice model for government departments wishing to demonstrate a high level of achievement in managing their information.[1]

IMA reports highlight areas of best practice and make recommendations for improvements. These recommendations will form the basis of an action plan against which progress will be tracked.

For more information about the programme and to view previous reports and action plans, see nationalarchives.gov.uk/information-management/our-services/ima.htm

Date: June 2012

[1] nationalarchives.gov.uk/information-management/our-services/ima.htm

Contents

1 Key findings of the assessment

1.1 The assessment team notes the progress the Ministry of Defence (MOD) has made since the 2009 spot IMA conducted by The National Archives. In the last two years, a departmental Information Strategy (MODIS) has been produced that is clearly aligned to departmental objectives, governance structures have been developed and the profile of the department's records and information management agenda has been raised. MOD is to be commended for these efforts and for the development of the departmental Records Management Improvement Plan. The pace must be maintained, however, if MOD is to achieve the demanding targets it has set itself.

1.2 Effective operations are dependent on the right information getting to the right people at the right time. A continued focus on records and information management will see MOD well-placed to achieve its goal of efficient information exploitation, while ensuring it can be fully accountable for its actions.

Governance and leadership

1.3 The Records Management Improvement Plan has been developed to halt a recognised decline in the standards of record-keeping within the department. Together with MODIS, the plan has the potential to transform MOD's records and information management performance. Consistent support for the chief information officer's (CIO) agenda is required across the department, and from individual top-level budget (TLB) holders in particular, if the required accompanying cultural changes are to be achieved.[2] The varied representation of responsibilities evident in individual TLB information strategies indicates that a uniform level of understanding has not yet been reached.

1.4 The new Electronic Document and Records Management System (EDRMS) and continued Defence Information Infrastructure (DII) roll-out collectively have

[2] MOD's command and management structure comprises Head Office together with process owners, senior responsible owners and a series of TLB holders, among whom the operating costs of Defence are allocated.

the potential to ease the burden on staff, but will not in themselves raise standards. MOD needs to factor records management principles into relevant communications and continue to emphasise adherence to centrally authored records management policy. This will help ensure that the system is used as required and that necessary audit trails are preserved.

1.5 Potentially robust governance structures for records and information management are in place at a local level. However, MOD is a large, complex and diverse organisation and the central CIO organisation is small. This makes oversight difficult. MOD must give serious consideration to the capability needed to provide assurance to the board.

1.6 Electronic records metrics are under development. These are necessary to enable objective measures of performance, centrally and at TLB and unit level. With these in place CIO will be able to objectively target areas of good and bad practice. CIO must give consideration to the need to measure the quality as well as the quantity of records that are being created. This will help MOD assure itself that a full and accurate record of departmental activity is being preserved.

1.7 MOD has developed a records management risk register and now includes information risk on the main departmental risk register. However, understanding of wider information risk was found to vary across the department, with some areas placing more emphasis on technology-related risks and risks to personal information. MOD must continue its work on information risk, driving a more consistent approach. This will allow risks stemming from a failure to manage and exploit information and records to be surfaced and mitigated.

1.8 MOD has widened its definition of information assets to include business critical information. This is commendable but the definition is not yet well understood. Information asset registers are a potentially valuable tool that allow the identification and management of risks to key assets and enable their effective exploitation. MOD must assure itself that the new definition and the department’s use of information asset registers supports the achievement of these goals.

Records management

1.9 With the introduction of the Records Management Improvement Plan, MOD recognises and intends to halt declining standards of record-keeping within the department. The introduction of a 'what to keep' approach is a pivotal element of the plan and will enable clear definition of those records that need preserving. Support and buy-in at TLB and unit level is necessary to ensure the right definitions are arrived at and that records are created as required.

1.10 Failure to declare records in line with policy puts MOD's corporate memory and ability to discover a single narrative of events at risk. This is of particular concern within operational areas, where staff may value information and understand the need to exploit it but see the creation of records as a separate enterprise or inconvenient extra step.

1.11 Work was under way in a number of locations visited to address the specific risk of unavailability or loss of information and records due to personal drive use. However, the assessment team found evidence that records are not yet being declared consistently and as a matter of course. At the same time, some staff were unclear what constitutes a record and expressed the view that all information can and should be retained. This approach is not sustainable, as the Records Management Improvement Plan makes clear. Together with inconsistent application of retention periods, it raises the risk that key information and records will be kept for too long or will become difficult to find.

Access to information

1.12 MOD's unsatisfactory performance in answering Freedom of Information requests led to monitoring by the Information Commissioner's Office between April and September 2011. Performance across the department had improved sufficiently by February 2012 for period of formal monitoring to cease. A clear priority was placed on this issue at a senior level, which may suggest an effective approach for improving performance in records and information management across MOD.

1.13 The warning, advice and reporting point (WARP) process for reporting data loss includes provision to record the context of incidents. A more consistent approach to this reporting, especially in terms of recording relevant disciplinary action, would allow clearer understanding of whether losses are happening because of a failure to follow policy or despite adherence to it.

Compliance

1.14 Information Managers (IMgrs) and other staff with records and information management-related roles within units do not always understand their responsibilities, and managers are not always supportive. TLBs should champion and prioritise such roles to ensure that their importance is understood and that their value in monitoring and driving compliance with policy is maximised.

1.15 MOD is to be commended for the development of the Information Management Passport and for the energy with which it is being promoted. A new version is reportedly being developed to target senior staff specifically. MOD should ensure that a focus on achieving desired completion rates does not come at the expense of measuring understanding and driving learning.

1.16 A lot is expected of the new EDRMS in many areas without an understanding of the specifics of the system and the problems that it will (and will not) solve. Expectations must be managed. At a local level, information management planning must focus on the successful adoption and proper use of the system as well as its arrival.

Culture

1.17 While many senior staff recognised the 'pain' of a failure in records management, staff do not yet consistently recognise that information and records management is a core and necessary component of their roles. Clear and consistent communication is needed throughout the command chain, with managers leading by example, to ensure staff understand and accept the need to adhere to records management policy and principles.

1.18 Some areas, such as Permanent Joint Headquarters (PJHQ) and Private Office within Central TLB, described induction processes that sought proactively to factor in records and information management and systems usage. Wider adoption of this approach in areas where records are generated, including coverage of 'what to keep' principles as they are developed, would be a useful way of driving good practice as staff transfer between units.

2 Risk matrix

Indicative score drawn from the pre-assessment analysis, on-site interviews and evidence submitted:

Governance and leadership	
Strategic management	
Business objectives	
Management controls	
Resourcing	
Risk management	

Records and information management	
Creation	
Storage	
Appraisal, disposal and transfer	
Management of information	
Digital continuity	

Access to information	
FOI/Data Protection	
Re-use	
Security	

Compliance	
Staff responsibilities and delegations	
Policies and guidance	
Training	
Change management	

Culture	
Commitment	
Staff understanding	
Knowledge management	

Key to colour coding	
Best practice	
Good	
Satisfactory	
Development needed	
Priority attention area	

3 SUMMARY OF RECOMMENDED ACTIONS

These recommendations will form the basis of an action plan that will be monitored.

Ref	Summary Recommendation	Paragraph:
1	**MOD to ensure the departmental CIO can mandate minimum levels of compliance:** • Key requirements outlined in the MOD Information Management Information Strategy (MODIS) and Records Management Improvement Plan must be represented consistently by Top Level Budgets (TLBs). • MOD to ensure TLBs actively drive engagement with CIO objectives at unit level, with middle management in particular co-opted into supporting and promoting the need for compliance to their staff. • TLBs and CIO to define escalation routes in cases of non-compliance with records and information management policy.	
2	**CIO to work with TLBs to manage and drive the culture change that will accompany the new EDRMS, factoring in lessons learned from current barriers to Meridio usage:** • MOD to review and refresh its EDRMS communications plan, with a focus on key stages and developments. • CIO to review role definitions for staff with local records and information management responsibilities. • CIO to ensure guidance relating to the new EDRMS explicitly refers to records and information management principles, policy and specialist information management staff roles. • TLBs to ensure that information planning focuses on driving proper use of the EDRMS as well as its arrival.	
3	**MOD to ensure that CIO has the capability to assure the board on progress against the department's records and information management objectives.**	
4	**TLBs to champion and prioritise the roles of staff with local records and information management responsibilities:** • TLBs to ensure the function of such staff in monitoring	

	and driving compliance with policy is recognised, developed and supported at unit level, particularly by middle management. • CIO and TLBs to assess the benefits of an intranet-based forum for key information management staff, to enable sharing of best practice and discussion of common issues. • TLBs to require business units to ensure staff appointed to such roles are familiar with central records and information management policy.	
5	**MOD to ensure the Information Management Passport reflects current strategic aims, and continuously measures staff understanding:** • MOD to consider developing a further questionnaire for information management staff, in conjunction with the proposed questionnaire for senior staff. • MOD should assess how to address performance if results identify downward trends in staff understanding.	
6	**CIO to ensure metrics provide local and central oversight of performance in information storage and records creation, with a view to sharing best practice and targeting areas of concern:** • CIO to assess what performance statistics are required from the new EDRMS and ensure that these are factored into its design. • CIO and TLBs to use the agreed performance information to drive up performance in creating key records in line with policy. • CIO to define how these metrics can be used to provide qualitative measure of performance, for example in conjunction with internal IMAs and information surveys.	
7	**Until the development of core metrics, CIO and TLBs to use available information to identify and prioritise business areas generating information with high value that are not declaring records:** • TLBs to review available statistics on personal drives, Meridio, SharePoint and New Technology File System (NTFS) and how they can be used consistently and effectively to demonstrate adherence to records and	

	information management policy. • TLBs to prioritise business areas where Information Managers (IMgrs) are absent. • TLBs to ensure that information not transferred to the EDRMS and orphaned is identified, risk assessed, and managed until a long-term decision on ownership or disposal is made.	
8	**MOD to address the varied understanding of information risk and its visibility at board level, ensuring it is consistently logged and managed and that distinctions between information and technological risks are understood:** • MOD to align more closely the individual TLB CIO and senior information risk owner (SIRO) roles. • MOD to drive a more consistent understanding of its appetite with regard to records and information-management-related risk, so that each TLB understands how this is applied to their business objectives. • CIO to ensure that all TLBs represent wider information- and records-related risks in local risk registers.	
9	**MOD to ensure the current definition of information assets meets business needs and that information asset registers enable effective management, including related risks:** • CIO to identify and implement a single template for TLB information asset registers or mandate inclusion of core criteria. • TLBs to ensure that the Cabinet Office information asset definition is clearly communicated, for example in terms of business continuity, and reflected in relevant documentation. • CIO to access digital continuity guidance published by The National Archives and ensure risks to information assets, such as technological dependencies, can be captured.	
10	**MOD to provide clarity and guidance on storage of information on allied systems and UK joint systems:** • Ensure policy clearly states ownership of information on creation, parameters for sharing information and responsibility for that information should operations cease or information is no longer required.	

11	**MOD's 'what to keep' policy and guidance to include input from TLBs, ensuring the right records are identified, created and that retentions periods are applied consistently:** • TLBs to underline the importance of implementing retention schedules to all staff. Monitoring and reporting of their application to be done by IMgrs. • CIO to assess the benefits of wider application of initiatives to deliver common file plans beyond the mandatory two-level defence file plan. • MOD to assess the benefits of creating an expanded and comprehensive 'what to keep' schedule for deployment in operational space, in addition to the high-level version already in place. • CIO to strengthen the wording of its guidance on minute-taking to ensure the risks of not taking full minutes are clear. • CIO to ensure that disposal schedules for Permanent Secretaries and Ministers are implemented fully after changes in key personnel.	
12	**CIO to assess the benefits of tighter controls where behaviours are having a negative impact on records creation:** • TLBs to reinforce at unit level the message that any changes to team site structures can cause links to records to be broken. • CIO to consider an appropriate technical size restriction on personal drive capacity, according to business area need. • MOD to ensure that the Defence Judicial Engagement Policy (DJEP) archive is not used for records storage in preference to the EDRMS.	
13	**The Corporate Memory Records (CMemR) team to revisit, with The National Archives, the status of records held by historical branches for selection for the public record.**	
14	**TLBs to ensure priority is given to provision of training for staff with records and information management-related roles, including Data Protection Officers:** • TLBs to ensure that staff in records and information	

	management roles not yet using the new EDRMS are trained to discharge duties and able to comply with central policy, including those who are still using NTFS. • CIO to ensure that sufficient training places are available.	
15	**TLBs to ensure that the context of incidents of information loss or mishandling is visible to the centre:** • TLBs to ensure that managers, without exception, record all context, including any disciplinary action taken, relating to incidents of information loss or mishandling. • TLBs to ensure that responsibility for recording such context is continued by relevant line managers until the investigation is completed.	
16	**CIO to review the information management protocols and guidance produced for staff to ensure they reflect CIO priorities:** • MOD to ensure that key risks highlighted in the records management risk register, Records Management Improvement Plan and MODIS are clearly addressed. • MOD to ensure that themes are cross-referenced consistently across the IM protocols.	
17	**MOD to ensure common standards in induction and leavers processes across the department:** • TLBs to ensure records and information management and system-specific instruction are included in induction training for staff expected to generate records. • TLBs to ensure that such training introduces the core information each unit handles, including information assets and 'what to keep', where to store records and information and how and why retention is applied. • CIO to develop strategies for knowledge capture to support TLBs succession planning and manage the risks of knowledge loss in priority areas.	

4 Summary of good practice

The following have been specifically identified as examples of good practice in this report.

1	**The MOD Information Strategy (MODIS) receives prominent senior-level endorsement** from the Permanent Under-Secretary of State and the Vice Chief of Defence Staff. This underlines the importance of the strategy to the department. MODIS establishes the Defence Information Vision and its status as an enabler of the main Defence Vision. It clearly establishes information as a strategic asset and the critical need for the department to transform the way it exploits it.
2	**MOD has introduced the CIO Forum as a means of implementing MODIS.** The existence of this forum has the potential to allow the CIO agenda to be clearly communicated across what is a large, complex and diverse department.
3	**MOD has developed the Defence Information Management Passport** consisting of a learning tool and the Defence Information Management Skills Maturity Model (DIMSMM) questionnaire. This is being proactively rolled out according to business need across the department, raising awareness as a result. A separate component specifically targeting senior staff and their responsibilities is under development.
4	**MOD has broadened its definition of information assets.** As this definition is embedded, MOD will be able to ensure better management of key business critical information in addition to personal information.
5	**MOD has produced the Records Management Improvement Plan to address declining standards in record-keeping.** This extends to consideration of cultural aspects and centres on the introduction of a

	‘what to keep’ approach to provide clarity on records creation.
6	**Staff in PJHQ has taken a particularly proactive approach to tackling the issue of records storage within personal drives.** ‘Naming and shaming’ has been used to drive improvements and statistics are displayed publicly. This approach should be considered as an option more widely.
7	**The CMemR team has demonstrated proactive engagement on the issue of continuity of digital information.** The team has engaged with The National Archives and invested considerable energy in raising related issues relating to the DII programme roll-out with the supplier, Atlas.
8	**A number of areas, including PJHQ and Private Office within Central TLB, have been proactive in including records and information management and systems use as a component of induction.** This ensures staff are aware of good practice from day one.

5 Highlights and areas for Improvement

Governance and leadership

Strategic management

5.1 The MOD Information Strategy (MODIS) covers the period 2009–14, superseding the previous Defence Information Strategy, which was issued in 2000. MODIS has prominent senior-level endorsement via a joint foreword by the Second Permanent Secretary and the Vice Chief of Defence Staff. This underlines the importance of the strategy to the department and **is an example of good practice.** The strategy is intended for biennial review; this was under way at the time of the IMA.

5.2 MODIS establishes the departmental Chief Information Officer (CIO) as Defence Operating Board lead on information matters, with responsibilities cutting across the department's top-level budget (TLB) structure. MODIS also establishes the departmental CIO as the process owner for information management, and underlines the need for support from other process owners and TLB holders.[3] The strategy outlines specific requirements, including the need for TLBs and process owners to produce their own information strategies.

5.3 The assessment team was supplied with copies of the 2011 Permanent Joint Head Quarters (PJHQ) Information Strategy, issued by the Chief of Staff (Joint Warfare Development), and the 2010 Navy Command Information Strategy, which contains a foreword by the Deputy Commander in Chief (DCIC). The authorship of these documents demonstrates senior level buy-in to and endorsement of the department's information management agenda within these TLBs. However, terminology and language used varies between the two documents along with the depth and quality of coverage of TLB responsibilities as defined in MODIS, such as the need to adhere to departmental standards for records capture and management. This variation may impact on the consistency with which priorities outlined in MODIS are communicated and understood across the department. **See Recommendation 1**

[3] Ten senior staff are appointed as process owners to ensure that specific activities are carried out with consistency and coherence across the department.

5.4 Although the visibility and authority wielded by the departmental CIO role has increased since the 2009 spot IMA conducted by The National Archives, MOD's size and complexity has placed limits on the extent to which the central CIO organisation can monitor and direct behaviours. The departmental CIO's remit is wide and he does not himself directly 'control all of the information levers of power', being reliant on TLBs to drive compliance with policy and the achievement of MODIS's goals.[4] Firm and consistent leadership is therefore required from TLBs on records and information management. The CIO Forum, chaired by the departmental CIO and attended by TLB CIOs, is an important development. Nevertheless, MOD must ensure that the departmental CIO is empowered to mandate minimum levels of compliance if the goals of MODIS are to be achieved. In particular, key requirements outlined within MODIS, such as the need to adhere to departmental standards for records capture and management, must be clearly established by TLBs. **See Recommendation 1**

5.5 MOD has developed a Defence Records Management Improvement Plan in response to a request from the Minister of State for the Armed Forces. The plan focuses on new rather than extant records, and is intended to halt a recognised decline in the standards of record-keeping across the department via a targeted action plan. The plan will receive strategic backing from the CIO Forum and will be supported by the MODIS Executive Group as part of the implementation of MODIS. Successful implementation is expected to bring benefits in terms of openness, transparency and accountability, but the plan also recognises that buy-in from senior management and from individual TLBs will be crucial to its success. **See Recommendation 1**

Business objectives and technology

5.6 MODIS establishes the Defence Information Vision, which is the

'Agile exploitation of our information capabilities to improve effectiveness and efficiency on operations and in support areas through access to, and sharing of, timely accurate and trusted information.'

5.7 The Defence Information Vision is described as a key enabler of the overall

[4] MOD Information Strategy, 2009.

Defence Vision. MODIS also recognises the actual and potential value of the information held by the department and the critical need for MOD to transform the way it exploits it. Information is identified as a strategic asset and the need to manage it accordingly is underlined in both MODIS and the PJHQ and Navy Command Information Strategies. **This is to be commended.**

5.8 MOD is midway through a long-running programme to rationalise the department's technological environment via the Defence Information Infrastructure (DII) programme. The programme seeks to bring the department onto a single operating system with standardised software. The next iteration of DII, Blenheim, will bring the staggered introduction of an updated Electronic Document and Records Management System (EDRMS) comprising Meridio Enterprise Data Capture (Meridio EDC) and Microsoft Office SharePoint Server 2007 by 2014.

5.9 MODIS suggests a causal link between historically low levels of technological investment and poor performance in information management terms. The DII programme is positioned as an enabler that will drive improved standards through increased levels of interoperability. This emphasis is reflected in the representation of the introduction of the new EDRMS as a key strategic milestone. However, while technological improvement has the potential to ease the burden, it will not in itself improve behaviours and culture where records and information management are concerned. MOD must ensure that TLBs place weight on acceptance and proper adoption of the new EDRMS. They must also proactively drive compliance with central records and information management policies and procedures. MOD should also ensure that guidance relating to the new EDRMS draws on and acts as a vehicle for best practice in records and information management. **See Recommendation 2**

Resourcing

5.10 Records management policy is the responsibility of the Corporate Memory Records (CMemR) team within the central CIO organisation. The team consists of three staff. At the time of the IMA, the TLB structure was under review following the publication of the Defence Reform report under the Strategic Defence and Security Review. The assessment team understand that the CMemR team may be subject to restructuring as a consequence. MOD must give serious consideration to the capability needed to monitor, report on and address departmental record management performance. **See**

Recommendation 3

5.11 The management of records and information is supported at unit level by a series of specialised roles. These include senior information officers (SIOs), who have overall responsibility and accountability for the records and information under their control; information managers (IMgrs) who implement information management and ensure compliance with records management policy; and information support officers (ISOs) who each head up an Information Hub (iHub). Information support administrators within the iHubs are responsible for ensuring effective receipt, distribution, archiving and disposal of information and records.

5.12 Two IMgrs interviewed in separate locations stated that they were not familiar with records and information policies. The assessment team also found limited evidence of interaction with the CMemR team, although the records management policy (JSP 441) identifies IMgrs as the primary point of contact at unit level. These roles provide a potentially robust means of driving adherence to policy and enabling the achievement of strategic aims including the objectives of the Records Management Improvement Plan. It is crucial that TLBs and units ensure staff with records and information management responsibilities are working to consistent standards. **See Recommendation 4**

Management controls

5.13 MOD has introduced a Defence Information Management Passport, comprising the Information Matters e-learning package and the Defence Information Management Skills Maturity Model (DIMSMM) questionnaire which requires a set score to pass. TLBs have set their own targets for completion, allowing them to take local business need into account. MOD expects units to achieve level 2 compliance with the DIMSMM by December 2012. **MOD is to be commended for the development of this tool.** However, the assessment team were informed that results are not collected in a manner that allows the identification or analysis of local or global themes. Statistics related to completion rates and scores could provide CIO with valuable insight into potential areas of weakness and good practice. **See Recommendation 5**

5.14 Despite a commitment by the CMemR team to conduct three or four internal IMAs per year, none were conducted in 2011 as staff were required to prioritise development of the Records Management Improvement Plan. The role of these

IMAs in driving improvement and sharing good practice may be at risk. **See Recommendation 3 and 6**

5.15 IMgrs are responsible for monitoring records and information management performance at unit level. However, the range of objective measures available appeared limited, with IMgrs referencing monitoring personal drive sizes and receipt of warning messages on team site capacity. Action taken was also found to vary. When asked how improved understanding among staff was measured, IMgrs referred to numbers of Information Management Passport questionnaires completed and increased numbers of staff asking questions.

5.16 The Records Management Improvement Plan includes a requirement for the development of electronic records metrics to assess record storage activity. In developing these, CIO should consider both what assurance it requires at TLB and departmental level and what metrics would enable IMgrs to objectively measure and benchmark the performance of their own units. Attention must be given to qualitative as well as quantitative measures. Without considering the quality of records that units are creating, MOD cannot be confident that the right information, such as the context surrounding key decisions, is being kept for as long as it is needed. At the same time, retention of unnecessary information may make vital information difficult to find and prevent its exploitation. In the short term, the identification of performance indicators that can be applied to the current information landscape should be regarded as a priority in light of the staggered EDRMS roll out. Where statistics are already available, for example on Meridio usage, MOD should make use of these. MOD must also decide what metrics are required from the EDRMS and ensure that they are factored into its design. **See Recommendations 4, 6 and 7**

Risk management

5.17 The HMG Information Assurance Maturity Model is in use within MOD and the department seeks to achieve Level 3 compliance by April 2012. The departmental information risk policy and the records management risk register provide evidence that information risk in its widest sense is being considered within MOD. The latter was implemented in October 2009 with the endorsement of the departmental records officer (DRO) and raises records and information-related risks affecting the whole department, including risks stemming from failure to follow policy and failure to capture and manage vital

records. **MOD is to be commended for the introduction of this register.**

5.18 Since the 2009 spot IMA of MOD, an information risk component has been added to the main departmental risk register. The assessment team was unable to view this but was informed by interviewees that the focus at board level is on risks relating to the safeguarding of personal information. MOD must ensure that wider information risks, such as those on the records management risk register, are also visible at this level. **See Recommendation 8**

5.19 Information risk registers are in use separately at TLB level. The collated top three information risks from each TLB are raised annually to the Defence Audit Committee. In parallel to the varied treatment given to strategic aims in TLB information strategies, coverage of information risk was found to vary across individual TLB risk registers and the combined risk register. Some TLBs such as Navy Command appear to have embraced a wider definition of information risk including, for example, impacts of failure to exploit and use information. However, in other areas assessment of risk focused more narrowly on technology or the handling of personal information.

5.20 The CIO Forum has responsibility for directing mitigation of high level information capability risks. Responsibility for information assurance falls to a network of TLB senior information risk owners (SIROs), with the departmental CIO in his capacity as MOD SIRO assuming ultimate responsibility for all information risk within the department. Absolute clarity is needed on the point at which SIROs escalate information risk. This is crucial to ensuring a consistent approach across the department. **See recommendation 8**

5.21 The assessment team has since been advised that the Defence SIRO has published a risk appetite statement to TLB SIROs on when to escalate information risks.

5.22 Within TLBs, the SIRO and CIO roles were often, but not exclusively, held by the same individual. A closer alignment of these roles would allow a more unified approach to information assurance and wider information risk. It would also be beneficial to the department as it works to develop its understanding of its information assets. **See Recommendation 8**

5.23 In the aftermath of the 2008 Data Handling Review, MOD's focus has been predominately on identifying information assets towards securing personal information. MOD is currently in the process of expanding its definition of information assets to encompass non-personal information with value to the department. **This represents a good start** although the expanded definition is not yet embedded.

5.24 The assessment team was told that units should now be using IARs to identify all important information that they are creating. A number of staff within MOD were aware of this change in emphasis, but little understanding was found of what it might mean in practice or what type of information was covered. Within PJHQ, the assessment team found concern that the wider definition of information assets could not be applied as all the TLB's information is 'business critical'. Information Asset Registers offer a potentially robust means of surfacing and managing a wide spectrum of risks to, and originating from, information assets. This can be done via the register itself or by establishing links, for example to an IT asset register. Drawing on The National Archives' digital continuity guidance, CIO must ensure that its definition of information assets and use of Information Asset Registers enables the efficient management of personal and business critical information. CIO must also work with TLBs and information asset owners to ensure definitions and requirements are understood. **See Recommendation 9**

Records and information management

Systems and storage

5.25 The number of systems and platforms in use within MOD can make sharing information difficult. Technological barriers exist between those with and without the current version of the departmental EDRMS, those on Defence Information Infrastructure Future (DII/F) and DII Maritime Deployed platforms, those still using the legacy New Technology File System (NTFS) and those using team sites. Other problems highlighted by staff included difficulties getting information on and off legacy systems, exchanging information with those serving overseas and sharing sensitive information with other government departments. Concern was also expressed over a lack of clarity surrounding ownership and sharing of information created on Nato and allied systems and using Foreign and Commonwealth Office servers. This is a significant issue given the potential sensitivity of the information in question, and consideration must be given to the impact and applicability of UK Freedom of Information (FOI) legislation and European law. **See Recommendation 10**

5.26 At the time of assessment, several units were in the process of creating or migrating material into new file plans ahead of the introduction of the new EDRMS. Staff interviewed during the visit to HMS *Diamond* stated that they were working with colleagues on HMS *Illustrious* to develop a common file plan beyond the mandatory two levels of the Defence File Plan, as both were in the same battle group. This could enable a coherent approach to records and information management. MOD should assess whether such initiatives have wider application within the department. **See Recommendation 11**

5.27 Where a NTFS solution is in place, staff have not always followed instructions to separate work in progress and records. This increases the likelihood of a confused structure, making information with long-term value difficult to find, and consequently harder to use and to protect. One interviewee described their old structure as ‘chaotic’ and ‘like a rabbit warren’, stating that they were frequently unable to find information they needed. In practical terms, not separating records has an impact on the ease with which material can be migrated into new file plans. In one location within Navy Command, the assessment team was told of a decision to draw a line under the information held in the NTFS and save it to DVD. This is contrary to MOD policy. Where such decisions have

been taken MOD must ensure that records are visible and information is clearly owned. **See Recommendation 7**

5.28 In two locations visited, staff stated that the idea of utilising the Defence Judicial Engagement Policy (DJEP) archive in preference to Meridio had been discussed because it was thought to have a superior search engine. Such action would raise the risk of duplication and impact on the ease of discovering a single narrative of events. If records are not created within the corporate repository there is a risk that key information will be lost or insufficiently protected with a serious knock-on effect to any subsequent enquiry. This is a message that MOD must continue to emphasise to staff now and as the new EDRMS is rolled out. **See Recommendations 1, 2 and 12**

5.29 A number of areas visited were reportedly tackling the problem of records storage within personal drives. iHub staff with responsibility for Parliamentary Branch had, for example, identified 1GB worth of information of which some 250MB was identified as records and saved to Meridio. Within PJHQ a proactive policy of 'naming and shaming' the worst offenders had been put in place to publicise the issue of records storage outside Meridio and drive people to review their personal drives. This approach may be of benefit to other areas of the department. However, unless statistics on personal drive size are actively sought from Atlas, storage issues and use patterns may not be obvious to local information management staff. MOD would benefit from tighter governance over personal drives and wider application of the proactive approach to monitoring demonstrated at PJHQ. **See Recommendations 7 and 12**

5.30 Team sites are in use in a number of locations and, where implemented effectively, appear to be acting as an enabler for collaborative working. Size restrictions are in place to drive record creation within Meridio. However, capacity were found to vary from 2GB to 10GB in locations visited and the number of staff describing ongoing problems with full or nearly full team sites indicates that not all staff using SharePoint are following departmental policy and routinely declaring records. Where this is the case iHub staff may come under pressure to increase team site size. Regular record creation is crucial to ensuring MOD can provide an audit trail of actions. The reason for size restrictions must be understood at unit level and team site capacity must not

simply be increased because staff are not declaring records. **See recommendation 12**

5.31 Some interviewees suggested that staff were reluctant to commit records to Meridio because of a lack of time, clarity on the need to do so or trust in the system. Meridio was described as difficult to search and concerns were raised about perceived loss of or difficulty in finding records. In some cases this was thought to be due to broken links to records caused by alterations to team site file plans, a technological limitation of the current system. The ease of saving to the new EDRMS is expected to drive users away from other alternatives. However, MOD should consider lessons learnt from issues with team site and personal drive usage as well as the potential impact of negative attitudes towards Meridio on take up of the new EDRMS. These may be of direct benefit to local records and information management staff who are tasked with driving compliance with CIO-authored policy. **See Recommendations 2 and 12**

What to Keep

5.32 The introduction of The National Archives' 'what to keep' approach is a central pillar of the Defence Records Management Improvement Plan and, consequently, of MOD's efforts to improve standards of records management.

5.33 The Defence Records Management Improvement Plan states that the 'keep everything, for ever, just in case' approach to records and information management cannot be supported. The assessment team found evidence of this attitude in a number of locations, caused by a lack of clarity over what constitutes a record and a fear of inadvertently disposing of key information. Staff, including IMgrs, said it was preferable to try to keep everything, referencing, for example, the unlimited storage capacity of the EDRMS. The possibility of duplication was described as an inconvenience rather than a risk. Some local records and information management staff told the assessment team they responded to full team sites by declaring everything as a record, or everything over a year old. In Naval Historical Branch (NHB) a deliberate decision appeared to have been taken to hold on to information with one interviewee stating 'we translated dispose to keep'.

5.34 At the other end of the spectrum, failure actively and routinely to define records according to policy raises risks to MOD's corporate memory. This is of particular concern in operational areas that work with and hold significant

volumes of high-value information. While such areas clearly acknowledge the crucial importance of 'information' and its timely provision, some staff interviewed appeared to see records creation and Meridio use as a separate enterprise and an inconvenient extra step. The 'what to keep' approach has the potential to provide structure and clarity around records creation, while the development of metrics will enable the performance of individual units to be measured. In advance, CMemR should work with TLBs to target areas generating high-value information where records creation levels cause concern. **See Recommendation 7**

5.35 Little evidence was found of systematic use of retention scheduling for electronic records and subsequent disposal. The frequency with which MOD staff rotate makes the establishment of clear guidelines particularly important. iHub staff described encountering resistance from some subject matter experts (SMEs) when seeking authority to dispose of records. Getting engagement from SMEs could prove difficult, for example, if they were new in post and felt they lacked the necessary knowledge, leading to deferral of review and the decision to keep or dispose of the record. **See Recommendation 11**

5.36 The introduction of the 'what to keep' approach has the potential to provide structure and clarity, transforming records keeping within MOD. However, CMemR will only be developing the tools for TLBs to implement; support and buy-in from the TLBs and individual units will therefore be crucial to its success and consistent application over time. This is especially true in operational areas such as PJHQ with a regular turnover of staff and a high-pressure working environment. **See Recommendation 11**

Appraisal, review and transfer

5.37 Records transfers to The National Archives fell dramatically in 2011. The assessment team understands that this was in part due to the Records and Review team's move from CIO into the new Defence Business Services (DBS) organisation. DBS Records and Review is based in Portsmouth and implements policy on records appraisal and transfer under a service level agreement with CIO.

5.38 Approximately 80,000 of MOD's records are over the current 30-year period for transfer to The National Archives, do not have retention applied and are not

covered by a Lord Chancellor's Instrument. MOD is working to select and transfer those records most likely to be of interest. In light of the application of the 20-year rule this backlog is expected to double and will be made transparent to the public.

5.39 Naval Historical Branch staff and the MOD Records Team should work with The National Archives in re-visiting the records stored at NHB as some may now be suitable for transfer. **See Recommendation 13**

Private Offices

5.40 MOD Private Offices use Model 1 of the guidance for Private Office records management issued by the Cabinet Office and The National Archives. Model 1 is recommended from a risk management point of view and requires both Private Offices and business areas to ensure that records are captured and stored within departmental records systems. Records of Ministers and Permanent Secretaries can be of central importance in demonstrating how and why key decisions were taken. Consequently, records and information management practices within Private Offices can positively or negatively influence behaviours in the department as a whole.

5.41 The assessment team visited a Ministerial Private Office. The preference for paper-based working among senior staff means that high volumes of paper information are generated in the course of Private Office business. This presents a number of challenges. However, robust handling processes appear to be in place for the management of these records via an experienced and dedicated support team.

5.42 The management of digital information needs to be improved within Private Offices and clear retention schedules need to be applied. The DRO should ensure that a disposal schedule is in place for Permanent Secretaries and Ministers covering such media as notebooks, diaries and email accounts. These must be implemented following a change of personnel. **See Recommendation 11**

Continuity of digital information[5]

5.43 MOD has worked extensively and been proactive in its engagement with The National Archives' digital continuity project. The department requested an assessment in February 2011 and is currently working to address the resulting recommendations, clarify and establish responsibilities and produce a roadmap. The assessment team understands that the CMemR team has invested a considerable effort in raising the profile of digital continuity and records management concerns relating to DII roll-out with the supplier, Atlas. This process highlighted differences in interpretation that could then be resolved. **MOD should be commended for its work in this regard.**

5.44 MOD currently has no standard information asset register template. Redacted screenshots of the Land Forces register provided to the assessment team indicate that consideration is given to purpose, status, location and risk to the department (via impact level) and user numbers. MOD should ensure that such headings are included on all Information Asset Registers as standard across all TLBs, or mandate adoption of a single preferred template. This would enable greater consistency in information asset management, allowing the same issues to be surfaced across the department. MOD should also assess the benefits of further expanding its Information Asset Registers in line with The National Archives' Digital Continuity guidance. **See Recommendation 9**

[5] Digital continuity is the ability to use your digital information in the way that you need, for as long as you need. See http://www.nationalarchives.gov.uk/information-management/our-services/digital-continuity.htm

Access to information

Freedom of Information and Data Protection

5.45 MOD's timeliness in responding to FOI requests was being monitored by the Information Commissioner's Office (ICO) at the time of the assessment. MOD receives a high volume of FOI non-routine requests for information: 830 for the first quarter 2011/12. This was the second-highest volume for any Whitehall body behind MOJ, with a total of 81% requests answered within the required timescale.

5.46 Answers to FOI requests may have to be sought across numerous locations, systems and formats. The central FOI team is reliant on the diligence of individual SMEs and getting requests to the right people is therefore extremely important. The assessment team was informed that the FOI team has rethought its allocation process with meetings now held each morning to try to ensure requests are directed to best effect. **This is good practice.**

5.47 FOI-related processes reviewed by the assessment team appeared adequate. However, levels of understanding of the Freedom of Information Act and MOD's obligations under it varied across the department. FOI staff described negative reactions to requests and a lower perceived status in comparison to Parliamentary Questions (PQs).

5.48 The Permanent Secretary has made a public acknowledgement of the need to reach the ICO's minimum required level of 85% of requests answered on time by the end of September 2011. The assessment team was provided with a copy of a letter written by the Permanent Secretary to TLB holders underlining the significance of the Freedom of Information Act and the implications of non-compliance. The assessment team is pleased to note that in February 2012 the Information Commissioner wrote to the Permanent Secretary to confirm that formal monitoring by his office would cease following a significant improvement in the department's performance.

5.49 TLB holders must continue to give a clear message on the importance of the Act, to ensure that staff understand its legislative status and the need to handle requests promptly. This is important as evidence was found that some staff

believe that blanket exemptions can be applied. Consistency is important and MOD should ensure that all areas of the department track requests via the Access Information Toolkit and that standard processes are followed when redacting documents. In one area, redaction was reportedly conducted by a senior member of staff with sticky tape and in another, a member of staff reported that redaction was conducted on a stand-alone system with no record kept of what had been released.

5.50 Subject access requests are handled by a network of data protection officers (DPOs), some of whom sit within secretariats and who have varied levels of seniority. DPOs help inform the work of information asset owners, forming a key link in the risk assurance chain, and provide staff with training. However there was concern that some DPOs had not had relevant training and were uncertain about the correct process for handling subject access requests. **See recommendation 14.**

Reuse

5.51 The assessment team did not interview relevant staff. However, MOD makes material available under the Open Government Licence and is regulated under the Information Fair Trader Scheme. MOD's IPR personnel manage a range of trademarks and a scheme is in place to licence the re-use of images. The department has published 181 datasets and 23 descendent datasets on the data.gov website.

Security

5.52 MOD staff are frequently required to handle highly sensitive material. The application of protective marking is described in the Defence Manual of Security, JSP 440. The single platform solution and new EDRMS should ease some of the issues regarding secure sharing of information, allowing the consistent use of links rather than attachments. This will place an emphasis on the proper management of access permissions. Policy currently requires permissions to be allocated on a group basis and removed and added as part of the leavers and joiners process. A number of staff stated that these were difficult and time-consuming to keep on top of. One member of staff believed they had retained permissions to access and work within their old area of the file plan after changing roles and another was uncertain why they had gained access to another unit's file plan overseas. Within PJHQ the assessment team was told that teams were actively reviewing access permissions and

considering whether entire team sites needed to be locked down or just individual folders. **This is good practice.**

5.53 MOD uses the warning, advice, and reporting point (WARP) process for managing and reporting data loss. Incidents involving significant or sensitive losses and breaches are recorded centrally, allowing them to be further escalated if required. A standard form is in use which allows the context surrounding losses to be recorded including any subsequent disciplinary action taken against staff. However, the assessment team was informed that these details are not always added by line managers, especially when staff changes occur during an ongoing enquiry. If managers do not record this type of information, it will be difficult to ascertain whether losses are happening because of a failure to follow policy or despite adherence to it. **See Recommendation 15**

Compliance

Staff responsibilities and delegations

5.54 In a number of locations, local records and information management roles were not fully understood by those who held or had responsibility for them. In one unit, J3 within PJHQ, the IMgr post had not been filled following a transfer. A number of those interviewed recognised a correlation between the absence of this key role and a lack of clarity and direction in records and information management within the unit. J3 records will be highly relevant to understanding UK and allied actions in Libya and Afghanistan; any risk that poor information management practice may result in important records not being available is therefore a serious one.

5.55 The manner in which staff in different locations had been appointed to records and information management roles suggested that the importance of these roles is not always recognised. Staff stated that they had been given information management responsibilities 'along with any other job that doesn't fit in' or because they were the most junior member of staff or were perceived to be IT-literate.

5.56 The Defence Records Management Improvement Plan requires TLBs to mandate iHub roles by December 2012. MOD must ensure that these and other records and information management roles are understood as being of core importance to the efficient functioning of the department. Fulfilling such duties fully can be demanding and time consuming, particularly where staff work in high-pressure areas. Such areas may also be ones that generate high-value records where it is particularly important that staff adhere to policy and procedure. Units must choose the right people for records and information management related roles and ensure that their work is recognised and actively supported by management and staff in general if the department is to fully benefit from them. **See Recommendation 4**

Policies and guidance

5.57 The Defence Records Management Manual (JSP 441), last reviewed August 2011, is complimented by a separate Joint Service Publication (JSP 747), covering information management policy. CIO has also produced a series of short-form information management protocols which provide concise summaries of specific issues such as email management. Topics covered are

not necessarily included within JSP 441 itself; as such the protocols are understood to support and expand upon this document.

5.58 The protocols are potentially a useful resource for staff looking for an answer to a specific question and are a vehicle for highlighting good practice in specific areas. They have grown organically over time with new protocols written as a need becomes evident. In some cases, therefore, links have not been made and key issues have not been highlighted. For example, Protocol 046, covering protection of personal information, does not refer to protective marking or to information assets and information asset registers. CIO should review the information management protocols to ensure that guidance is consistent and focussed towards objectives defined in MODIS and the Defence Records Management Improvement Plan and addressing key known risks. **See Recommendation 16**

Training

5.59 The Information Management Passport was launched in summer 2010 with backing from the Second Permanent Secretary. It is intended to educate staff and raise standards in records and information management, demonstrating this via subsequent completion of the questionnaire component. Two locations visited (HMS *Diamond* and PJHQ) have made completion of the Information Management Passport mandatory before assumption of duties. This makes a clear statement and **is to be commended.**

5.60 Most staff interviewed were aware of the need to complete the questionnaire and the priority placed on achieving a pass by senior staff. This emphasis may, however, be counterproductive in some regards. A number of interviewees expressed concern that answering the questionnaire component honestly with regard to working practices resulted in receipt of a fail mark. As a pass was understood to be required, some staff had simply amended their answers to achieve this. The potential value of the Information Management Passport in measuring current behaviours and driving learning and directing staff to the guidance and support they need may therefore not be being fully realised. The use of one set of questions may also be problematic if it does not reflect the variety of systems that are in use and the ways of working that these demand.

5.61 CIO is in the process of refreshing the Information Management Passport and producing a separate questionnaire targeting senior staff**. MOD is to be**

commended for this. MOD should also consider whether further questionnaires could be targeted to staff with records and information management roles. **See Recommendation 5**

5.62 MOD offers records management training courses to all staff at the Defence Academy (formerly at RAF Halton) and undertakes outreach activities including road shows. Professional training courses are offered to records and information management staff. The assessment team was informed that there was currently a backlog of IMgrs receiving training. This was thought to be due to priority being placed on carrying out the 'day job' and staff not being able to attend scheduled courses as they are often oversubscribed. This view was particularly prevalent within operational areas where some staff described training as a luxury rather than a necessity.

5.63 The training package on offer is standardised for each role and a decision has been taken to include training on the new EDRMS The provision of one-size-fits-all training was, however, viewed as unhelpful by some of those staff still operating on a NTFS basis. Some units will not be receiving the new EDRMS for many months, and in the meantime information management staff need the tools to ensure that records and information management policies are adhered to. **See Recommendation 14**

Change management

5.64 Clear communication to key staff is needed to manage the expectation that is being attached to the introduction of the new EDRMS.

5.65 Interviewees at all levels expected the adoption of EDRMS to solve information management problems, but were not necessarily aware of the specifics of the new system. This was true of senior staff from HQ, iHub staff and end users. At the same time, interviewees expressed concern that they were championing the benefits of a system that has not yet been tested and which they had not yet had sight of. This lack of clarity was found to have an effect on planning within individual units. In one location, the assessment team was told that information management planning had not been re-evaluated because the tools were changing; in another, milestones had not been defined because of a lack of clarity on the EDRMS roll out.

5.66 MOD must though ensure that key staff are clear what changes the new system will bring and the required ways or working that will be needed. TLB holders need to be clear that technological improvement will not in itself drive better behaviour, but must be accompanied by culture change and a focus on adherence to records and information management policies and procedures. Attention must be given to supporting staff as they adapt to the ‘create once, use many times’ approach that the system will enable. At a local level, information management planning should focus on adoption and proper use and uptake of the new EDRMS as well as its arrival. **See Recommendation 2**

Culture

Commitment/staff understanding

5.67 The assessment team found greater awareness of the importance of records and information management than at the time of the 2009 spot IMA. The introduction of the Information Management Passport and statements from senior management in support of the departmental CIO's agenda have been instrumental in achieving this. In some areas, such as PJHQ, staff recognised a significant increase in understanding in the last few years. However, it was apparent that records and information management are still viewed as additions to, and even distractions from, the day job by some staff.

5.68 The Defence Records Management Improvement Plan emphasises several areas where cultural changes need to take place. These include minute taking in meetings, an area tested during the assessment. Staff interviewed were broadly confident that minutes were taken at important meetings and that audit trails would be available on key decisions where they were not. **MOD is to be commended** for highlighting this issue and should consider strengthening the wording of this point to ensure that the risks are fully understood. MOD should also ensure such considerations are factored in to 'what to keep' requirements as they are developed. **See Recommendation 11**

5.69 Senior staff interviewed spoke of the importance of records and information management and underlined the potential 'pain' of getting things wrong. This message did not always appear to be receiving the necessary support further down the management chain. MOD staff work in demanding and high-pressure environments and are subject to numerous competing priorities. If managers do not lead by example, promoting good practice and emphasising the importance of adhering to policy, staff working below them may not understand or accept the need to follow it. Clear direction is needed to staff that records and information management are a core part of their role, and that good practice in line with policy will benefit MOD. **See Recommendation 1**

Knowledge management

5.70 MOD uses specialist bodies such as NHB to ensure that the department can gain value from its records. Although several staff interviewed needed to work with records dating back to the Second World War, the focus for many is on the short term and present day. A number of interviewees also expressed concern

over knowledge loss in the face of staff turnover, including those with specialist knowledge. Within NHB itself the assessment team noted a lack of succession planning around key roles. **See Recommendation 17**

5.71 A lack of detailed knowledge of what has gone before may impact on the ease with which business areas can answer FOI queries and Parliamentary Questions, and also the extent to which units make use of their own records. Leavers and joiners processes are a key means of addressing these issues, allowing capture and transfer of knowledge. The assessment team found a number of **examples of good practice** in this regard. Within PJHQ there is an emphasis on inductions, with an expectation that records and information management are included and that staff will spend a week shadowing their predecessor. Information management staff at PJHQ also invested time in producing Meridio and ways of working guides. One area also reportedly provided a mandatory induction to team site usage.

5.72 While other areas such as Private Offices also described in-depth inductions, a number of staff reported having little or no handover or induction within their current business area. The extent to which records and information management or data protection featured was also found to vary. In one case a member of staff stated that the first time they had encountered the idea of information management was in the course of a briefing ahead of their interview for this assessment. In light of MOD's varied technological landscape, the provision of an introduction to the systems that are in use and ways that records and information should be managed as a component of inductions would be of benefit to the department and could be used to drive desired outcomes of the Records Management Improvement Plan. **See recommendations 1 and 17**

APPENDIX ONE: GLOSSARY

CIO	Chief Information Officer
CMemR	Corporate Memory Records team
DII	Defence Information Infrastructure
DII/f	Defence Information Infrastructure Future
DRO	Departmental Records Officer
EDRMS	Electronic Document and Records Management System
FOI	Freedom of Information
ICO	Information Commissioner's Office
iHub	Information Hub
JSP	Joint Service Publication
IMA	Information Management Assessment
IMgr	Information Manager
MOD	Ministry of Defence
MODIS	Ministry of Defence Information Strategy
NTFS	New Technology File System
PJHQ	Permanent Joint Headquarters
SIRO	Senior Information Risk Owner
SME	Subject Matter Expert
TLB	Top Level Budget

APPENDIX TWO: THE ASSESSMENT TEAM

The assessment was conducted by members of the standards department and specialist colleagues from The National Archives between 12 and 23 September 2011.

The assessment team comprised:

- Head of Standards
- Standards and Assessment Manager
- Standards and Information Policy Manager
- Standards Adviser
- Lead Information Management Consultants
- Information Management Consultants
- Information Security Architect
- Chief Executive (observer)

Assistance provided by MOD:

The assessment team is grateful for the cooperation and assistance of all staff at HQ, PJHQ, Navy Command HQ, HMS *Diamond*, NHB and Portsmouth Flotilla who were interviewed, provided additional information or facilitated the assessment process.

Our particular thanks are extended to the CMemR team for their organisation and hospitality.