

20 June 2008



# **MOD Action Plan in response to Burton Report**

20 June 2008

## **MOD ACTION PLAN IN RESPONSE TO THE BURTON REPORT**

### **Introduction**

1. This Action Plan has been produced by the Ministry of Defence in response to the report of the Sir Edmund Burton's Review of the loss of personal data by the Department. It addresses how all of the report's 51 Recommendations for how the Department should bring its handling of personal data to an acceptable state will be met.

### **Workstreams**

2. The Department's response to the Review is broken down into a set of workstreams as follows:

- a. Doctrine.
- b. Policy identification and development.
- c. Awareness.
- d. Training.
- e. Compliance and audit.
- f. Establishing the current baseline and then improving the data protection stance of existing projects
- g. Technology exploitation.
- h. Accreditation.
- i. Governance.
- j. Rectification of TAFMIS' areas of non-compliance with the Data Protection Act.

3. The main themes of the action plan are to:

- a. ensure that awareness of the importance of correctly handling personal data and the procedures for doing so are embedded across the Department at all levels;
- b. move the Department to a position of compliance with the Data Protection Act as soon as possible and then maintain that status;
- c. establish a rigorous regime of Audit, Assurance and Compliance for Data Protection;
- d. ensure that Top Level Budget areas and Trading Funds develop, resource and maintain adequate Data Protection capability within their organisations, including senior leadership.

## **Governance**

4. Programme oversight will be provided by the Defence Operating Board who will receive regular (3 monthly) reports of progress from DG Information who will lead the implementation of the Action Plan.

## **Action Plan structure**

5. The detail of the Action Plan is provided at Annexes A and B as follows:

- a. Annex A provides, in tabular form, a listing of the recommendations in the Burton report, with for each:
  - i. the desired outcome of the recommendation (these have been agreed with Sir Edmund Burton as a true reflection of the intent of his recommendations);
  - ii. a cross-reference to the tasks (in Annex B) that will deliver the outcome of the recommendation;
- b. Annex B provides a definition for each work stream of:
  - i. the tasks it comprises;
  - ii. due dates for each task;
  - iii. the Departmental lead responsible for overall delivery of the workstream;
  - iv. those in MOD accountable for the delivery of each task;
  - v. a cross-reference to the Burton recommendations that it supports.

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
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.	A system that is compliant with DPA and fulfils the business needs of all Services. Fully functional	J.1
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.	An MOD and Contractor community that understands key information, the obligations in records management, and the consequences of failure	C.6
3	Supervising officers to be rigorous in enforcement of security instructions.	Security instructions that are clearly understood with a means of measuring compliance to enforce them	E.5.1
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.	Stage 1. Improved project governance for TAFMIS  Stage 2. A governance process and structure representing good practice, with rigorous audit and compliance regime	J.5
5	MOD to review DPA retention policy to remove potential ambiguities and ensure clarity where variations exist.	Clear, unambiguous DPA compliant data retention policy that is communicated and rigorously enforced	B.3.1, C.4, E.4.1, E.5.3

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
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.	Transparent responsibilities for personal data management that are contractually enforceable and audited	B.3.7, B.4, C.6, E.4.8, F.7, I.3, I.4, I.9
7	Contractor to be tasked to cleanse TAFMIS data base as a matter of urgency.	Task EDS to cleanse TAFMIS database	J.4
8	MOD to show greater rigour in ensuring that system security procedures are enforced.	System Security Procedures that are clear, compliant and proven to be followed through audit	B.7, C.3.3, D.6, E.5.1, E.5.2
9	MOD to ensure that individual and corporate responsibilities under DPA 1998 are understood and complied with.	A Department where policy is compliant with DPA and where individuals (responsible officers and working level) understand their part in that policy	B.2.1, B2.2, B.3.1, B3.2, B.4.6, B.5, B.7, C.3, C.4, C.5, C.6, C.7, D.1, D.5 E (all), I.3, I.4, I.7, I.8
10	That all MOD organisations and business units report thefts and losses of removable media in strict accordance with JSP541.	All instances of removable media loss reported and acted upon, including through analysing and effecting follow through action	E.1

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
11	MOD to review and adapt established staff procedures and processes, taking account of the opportunities and vulnerabilities implicit in new ICT.	Business processes across the Department adapted to exploit the full benefits of IT, while ensuring that sensitive issues are addressed rigorously and assuring that information and data deliver full operational and business benefit	A.3
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.	Full and continuous visibility of the extent of the Department's data holdings	F.3, F.5
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.	Data holdings across the department that meet only the actual business need and are fully compliant with legislation, proven by audit and detailed within SIC	B.2.2, B.2.3, B.3.2, B.3.3, C.3.5, C.3.7, C.3.8, D.5, E.3, E.4.1, E.4.2, E.4.3, E.4.4, E.4.5
14	MOD to carry out a risk-benefit analysis on the requirement to hold large amounts of personal data to meet Centre tasking.	Holdings of information across the Department that are the minimum necessary to deliver business value	B.2.1, B.2.2, B.2.3, C.3, E.3, E.4.2
15	That MOD identifies and facilitates the sharing of good practices.	A learning Department that identifies and acts promptly to correct mistakes; remains alert to identify, adapt and adopt good practice; and encourage and reward innovation	B.3.4, B.6, C.3.4, C.3.6, D.4, E.4, F.6, G.4

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
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.	A clear statement that defines the value of information, the vulnerabilities to which it exposes the Department the behaviour that must apply across all areas that exploiting the value while mitigating the risks	A.1
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.	A Department where information value, exploitation and governance is understood and runs throughout business processes	C (all)
18	Information Risk to be addressed as a standing risk item on all Executive Boards and Audit Committees.	Information Risk considered by all relevant Executive Boards and Audit Committees	E.4.4, I.2
19	Mandated assurance processes analogous to those for Health and Safety to be introduced for Information Risk.	Information Risk to be addressed at all levels with the same degree of rigour accorded to Health and Safety	E.4.5, I.8, I.9, I.10
20	Information Risk to be formally assessed in Capability Reviews and in Office of Government Commerce (OGC) Gateway Reviews.	Information Risk assessed by all Capability and OGC Gateway Reviews	I.6
21	MOD to seek guidance from the Information Commissioner on the status of the TAFMIS database(s) as regards the Data Protection Act.	TAFMIS status understood	J.3

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
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.	All systems fully compliant through life with all legal and security regulations	I.4
23	Detailed accountabilities for Data Protection across the Department to be clearly articulated.	A Department in which policy is compliant with DPA and where individuals (responsible officers and working level) understand their accountability in delivering that policy	B.3.5, E.4.6, F.4, I.3, I.4, I.5, I.11
24	MOD to improve awareness and uptake of current Data Protection Act training.	A workforce that understands the universal importance of information governance and where specialists see themselves as directly or indirectly rewarded	D.1, D.2, D.5
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.	A Department in which information is held in one programme but used by many others with adequate dependency management and resilience, taking account of Data Protection legislation	B.3.6, E.3, E.4.7, G.3

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
26	MOD to produce clear policy on sharing personal data with third parties, including changes to standard contractual clauses as required.	Clear, compliant and enforced policy on sharing personal data outside the MOD	B.3.7, C.6, E.3, E.4.8, F.4, F.7
27	To instigate a full census of non-laptop removable media device holdings (including USB devices, CDs etc), in order to ensure that they are formally approved and accounted for on a routine basis.	Full visibility of all removable media across the Department	F.1, F.2
28	MOD to implement guidelines on the storage of personal data on these devices, including the requirement for encryption, as necessary.	Removable media holdings that balance business requirement against risk exposure, with effecting compliance and audit processes	B.1.2, C.3.3, E.3, E.5
29	MOD to reiterate, or revise, Departmental guidance on the use of private mobile media devices to process MOD data.	Clear, enforceable and risk assessed policy on the use of private mobile media devices	B.1.1, C.3.3, E.5
30	MOD to define the full scope of responsibilities for the Departmental Chief Information Officer functions.	A clear and accepted statement of Department CIO functional responsibilities that covers all areas of information risk	I.9.3
31	MOD to reinforce the authority of the MOD SIRO to act on behalf of the Defence Operating Board in respect of information risk.	Clear and recognised mandate for SIRO	I.8, I.9.3

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
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.	High degree of confidence in MOD and TLBs that information exploitation and protection are managed effectively in order to assure the confidentiality, integrity and availability of critical information and data	I.8
33	MOD to determine the level of risk it is prepared to bear in the area of accreditation, and resource the accreditors accordingly.	An efficient accreditation organisation that accurately assures through life information risk management with respect to systems so that the Department can manage risk appropriately	H.2
34	MOD to appoint a professional head of accreditation with MOD.	Clear ownership and mandate of accreditation task including the development and maintenance of essential skills across the Department with links to key private sector partners	H.1
35	Accreditors to receive appropriate training to enable them to address data protection issues.	An appropriately trained accreditation team that can effectively address data protection issues	H.3
36	MOD to consider adopting appropriate technological solutions to achieve compliance with data protection regulations.	Assurance that, through a combination of technological solutions and users behaviour, systems can only be operated in a safe manner	G (all)
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.	Only qualified users to be authorised to handle personal data	B.3.8, D.5, E.5.4

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
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.	A system that applies equitable censure to those that negligently or deliberately compromise personal information, while enabling the department to continue to learn and improve	I.12
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.	Clear, concise, compelling, useful user guide with longevity	B.5
40	Authoritative policy documents like JSP 440 to remain; but with 'break-out' documents on e.g. the latest technological developments accompanying them.	A policy framework that adapts to emerging solutions while maintaining a clear and consistent direction	B.5
41	MOD to implement the principle of storing and handling only the minimum amount of personal data required to carry out core business.	A department in which all systems and processes retain only the minimum information necessary for the business need	B.2.1, C.3.5, E.3, E.4.1

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
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.	An environment in which every decision on information useage takes account of the risk/benefit implications	B.2.2, E.3
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.	Clear, enforceable and risk assessed policy on the use of private computers	G.1
44	Urgent consideration to be given to offering free, safe, disposal of personal data devices.	A efficient arrangement to enable personnel to dispose of personal information holdings	G.2
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.	A Department aware of information risk and potential impacts on the business and of the available methods of mitigation	C3.1, C.3.2
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.	Heightened awareness of among senior leaders of current and emerging threats	C.2.1

#	Burton Recommendation	Outcome	Workstream Tasks (see Annex B)
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.	Heightened awareness of issues among all relevant MOD staff	C.2.2
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.	A comprehensive understanding across the Department the critical role played by information in delivery of British Defence Doctrine and the Network Enabled Capability	A.2
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.	Future training needs identified and resourced	D.1, D.2, D.3
50	Full use to be made of the Joint Training and Education institutions, such as the Defence Academy and proposed Defence Security School , in providing education and training in the effective exploitation and protection of information and data, including obligations under DPA 1998.	Effectively trained and educated staff across the Department, developing effective links with the National School for Government	D.4
51	Decisions on resourcing this initiative to be taken at Defence Board Level.	Sufficient funding for the essential transformational programme.	I.1

A. Doctrine - This is the process to ensure a comprehensive understanding across the Department of the critical role played by information in delivery of British Defence Doctrine and the Network Enabled Capability.			Departmental Lead for Workstream - DCDC	
Date Due	#	Task	Resource	Burton Recommendations Supported
30-Sep-08	1.0	Define and publish a clear statement that defines the value of information, the vulnerabilities to which it exposes the Department and the behaviour that must apply across all areas that exploiting the value while mitigating the risks for Information	DCDC, Defence Academy	16
31-Oct-08	2.0	Ensure that a comprehensive understanding exists across the Department as to the critical role played by information in delivery of British Defence Doctrine and the Network Enabled Capability	DCDC, DG Info	48
31-Mar-09	3.0	Ensure that process and procedures are in place to enable the Department to adapt to exploit the full benefits of IT, while ensuring that sensitive issues are addressed rigorously and assuring that information and data deliver full operational and business benefit by:	DG Info (lead)	11
	3.1	incorporating information security into the information management handbook	Info Expl	
	3.2	TLBs drafting Electronic Working Practice/Ways Of Working to capitalise on information governance opportunities and mitigate vulnerabilities	TLBs, TFCEs	
	3.3	effective communications plan to educate staff on the reasons behind better business processes	DG Info, TLBs, TFCEs	

<b>B. Policy - This is the process to deliver a policy framework that reflects current legislation and strategic requirements, balancing business requirements against risk exposure. It must be adaptable to emerging solutions while maintaining a clear and consistent direction.</b>			<b>Departmental Lead for Workstream</b> <b>- DG Info</b>	
Date Due	#	Task	Resource	Burton Recommendations Supported
	1.0	Confirm or revise Departmental policy/guidance/procedures on the use of:	D Def Sy	
30-Jun-08	1.1	private mobile media devices		29
30-Jun-08	1.2	removable media holdings		28
	2.0	Promulgate new policy/guidance/procedures on the following:	Info Access (lead)	
30-Jun-08	2.1	storing and handling only the minimum amount of personal data required to carry out core business through life	Info Access	9, 14, 41
30-Jun-08	2.2	a challenge process, based on balancing information risk with business requirement, for 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	Info Advisor, Info Access, DSSO	9, 13, 14, 42
30-Jul-08	2.3	defines the roles and responsibilities of Information Asset Owners	Info Advisor	13, 14
	3.0	Provide or refresh policy/guidance/procedures on:	Info Advisor (lead)	
30-Sep-08	3.1	information retention requirements to comply with the Data Protection Act	Info Access, TLBs and TFs	5, 9
30-Sep-08	3.2	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.	Info Access/Advisor with TLBs,TFCEs	9, 13
30-Sep-08	3.3	arrangements for "whistleblowing" and "amnesties" to assist in exposing vulnerabilities	Info Advisor	13
30-Sep-08	3.4	rewarding good ideas that are adopted as best practice	Defence Board (Info Advisor lead)	15
30-Sep-08	3.5	rectification of legacy programmes to comply with the Data Protection Act	Info Advisor, DSSO monitor, TLBs and TFCEs to implement	23

<b>B. Policy</b> - This is the process to deliver a policy framework that reflects current legislation and strategic requirements, balancing business requirements against risk exposure. It must be adaptable to emerging solutions while maintaining a clear and consistent direction.			<b>Departmental Lead for Workstream</b>  <b>- DG Info</b>	
Date Due	#	Task	Resource	Burton Recommendations Supported
30-Sep-08	3.6	making personal data accessible through secure links to central servers rather than locally	EC area, DE&S, DG Info, TLBs, TFCEs	25
30-Sep-08	3.7	secure and trusted sharing of personal data and provision of services with third parties, including changes to standard contractual clauses	DE&S	6, 26
30-Sep-08	3.8	minimum mandatory requirements for user training and certification to handle personal information	Info Access	37
30-Sep-08	4.0	Introduce policy/guidance notes that inform the Defence Industry of Departmental policy concerning the handling of MOD personal data by Contractors	Info Access, DSSO, D Def Sy, DE&S	6, 9
15-Dec-08	5.0	Introduce policy/guidance notes that provide short, accurate, readable and timely 'break out' updates to reflect changes in technology, legislation, strategy or policy which are then formally adopted into JSPs etc	Info Advisor, Info Access, D Def Sy	9, 39, 40
15-Dec-08	6.0	Create a centre of excellence within Defence responsible for maintaining, encouraging and monitoring best practice on personal data handling	Info Access, D Def Sy	15
31-Mar-09	7.0	Complete a review of JSP440 to remove ambiguities and ensure that Data Protection Act compliance is fully explained and that personal responsibilities are clearly laid out	D Def Sy	8, 9

<p><b>C. Awareness</b> - This is the process of informing the Defence Community about handling key information, the obligations in records management, and the consequences of failure with respect to handling personal data. Leading to a Department where information value, exploitation and governance is understood and runs throughout business processes with individuals (responsible officers and working level) understanding their responsibilities.</p>			<p><b>Departmental Lead for Workstream</b> <b>- DGINFO</b></p>	
Date Due	#	Task	Resource	Burton Recommendations Supported
30-Jun-08	1.0	Develop comprehensive awareness and communications plan	Info Access, DSSO, D Def Sy, DGMC	17
	1.1	define key messages		
	1.2	define stakeholder groups		
	1.3	define communications channels		
	1.4	define Measures of Success and performance monitoring process		
	2.0	Establish and brief threat picture		17
31-Jul-08	2.1	Senior briefing programme by national authorities for Senior Leaders and Managers (Defence Board Members)	2nd PUS, VCDS, National Authorities	46
31-Oct-08	2.2	Develop succinct version of threat picture for wide briefing arrange and cascade briefing programme through PSyA chain	D Def Sy	47
30-Sep-08	3.0	Prepare materials for awareness campaign covering	DG Info, DSSO, D Def Sy, DGMC	9, 14, 17
	3.1	the importance of information and its protection	Info Access, DSSO, D Def Sy, DGMC	45
	3.2	risks and mitigations	Info Access, DSSO, D Def Sy, DGMC	45
	3.3	the revised policy framework	Info Access, DSSO, D Def Sy, DGMC	8, 28, 29
	3.4	the "whistle-blowing" process	Info Advisor/Access	15
	3.5	data retention and storage	Info Access, DSSO, D Def Sy, DGMC	13, 41

<p><b>C. Awareness</b> - This is the process of informing the Defence Community about handling key information, the obligations in records management, and the consequences of failure with respect to handling personal data. Leading to a Department where information value, exploitation and governance is understood and runs throughout business processes with individuals (responsible officers and working level) understanding their responsibilities.</p>			<p><b>Departmental Lead for Workstream</b>  - <b>DGINFO</b></p>	
Date Due	#	Task	Resource	Burton Recommendations Supported
	3.6	capturing and rewarding best practise	Info Access, DSSO, D Def Sy, DGMC	15
	3.7	individual responsibilities and accountabilities	Info Advisor	13
	3.8	governance processes	Info Advisor	13
15-Dec-08	4.0	Deliver campaign to raise awareness (end date 31 Mar 09)	DGMC, Info Access, DSSO, D Def Sy, TLBs, TFCEs	5, 9, 17
Ongoing	5.0	Monitor and manage effectiveness of awareness campaign	DGMC, Info Access	9, 17
15-Dec-08	6.0	Define the categories and characteristics of key information to enable MOD and Contractor community to understand their obligations in records management, and the consequences of failure	Info Access, DSSO, D Def Sy, TLBs, TFCEs	2, 6, 9, 17, 26
31-Mar-09	7.0	Embed data handling awareness in routine training	Info Access + training delivery organisations (Defence Academy, dblearning, da learning, and proposed Defence Security School)	9, 17

<b>D. Training - This workstream intends to develop the training to ensure that individuals (responsible officers and working level) understand their part in compliance with the Data Protection Act and have appropriate skills and competences</b>			<b>Departmental Lead for Workstream</b>  <b>- DG Info</b>	
Date Due	#	Task	Resource	Burton Recommendations Supported
31-Jul-08	1.0	Review all the current education and training on the effective exploitation and protection of information and data delivered across Defence and identify uptake	Info Access, dblearning and training delivery organisations (Defence Academy, dblearning, da learning, and proposed Defence Security School), TLBs, TFCEs	9, 24, 49
31-Aug-08	2.0	Set training targets	Info Access	24, 49
30-Sep-08	3.0	Identify future needs	Info Access	49
15-Dec-08	4.0	Plan and develop training resources based on:	Info Access	15, 50
		a clear appreciation of the differing levels of training required to enable understanding at awareness, practioner and expert levels		
		maximum use of the Joint Training and Education institutions, such as the Defence Academy and proposed Defence Security School		
		identifying ways of motivating/incentivising uptake in training		
		the possible benefits of employability for those who understand information governance (certification, private sector recognition?)		
		communicating policy & Doctrine as part of core training		
		ensuring that training and policies are in place to enable controlled access by qualified personnel only (including contractors)		

<b>D. Training</b> - This workstream intends to develop the training to ensure that individuals (responsible officers and working level) understand their part in compliance with the Data Protection Act and have appropriate skills and competences			<b>Departmental Lead for Workstream</b>  - DG Info	
<b>Date Due</b>	<b>#</b>	<b>Task</b>	<b>Resource</b>	<b>Burton Recommendations Supported</b>
31-Mar-09	5.0	Ensure that individual and corporate responsibilities under the Data Protection Act are understood and complied with by mandating awareness training for all in Defence on an annual basis	Info Access	9, 13, 24, 37
30-Jun-08	6.0	Deliver appropriate training to Accreditors to enable them to address data protection issues	DSSO (dblearning, Defence Academy, proposed Defence Security School)	8

<b>E. Compliance - This is the process ensuring through Governance, Audit and Assurance that the Department continues to be compliant with current and future Legislation, Policy and Guidance.</b>			<b>Departmental Lead for Workstream</b>  <b>- DG Info</b>	
Date Due	#	Task	Resource	Burton Recommendations Supported
30-Jun-08	1.0	Ensure that all members of the Department are fully aware of the requirements to report thefts and losses of removable media in strict accordance with JSP541 with specific focus on;	Info Advisor, DSSO, D Def Sy, TLBs, TFCEs	9, 10
	1.1	impact of data loss and the time taken to report an incident	Info Advisor, DSSO, D Def Sy, TLBs, TFCEs	
	1.2	clear statements detailed within Terms of Reference of relevant responsible officers	Info Advisor, DSSO, D Def Sy, TLBs, TFCEs	
	1.3	reporting requirements to be incorporated within TLMP and System Security Procedures	D Def Sy, DSSO	
	1.4	requirement for reporting is very clearly explained within mandated awareness and specific training	DSSO, D Def Sy	
30-Jun-08	2.0	Ensure guidelines are reiterated across Defence to ensure understanding on the storage of personal data on removable media, including the requirement for encryption, as necessary.	Info Advisor, DSSO, D Def Sy, TLBs, TFCEs	9
30-Sep-08	3.0	Put in place and maintain 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. This must include compliance and audit checks against the use of removable media with generic acceptable and unacceptable usage scenarios.	Info Advisor, Info Access, DSSO	9, 13, 14, 25, 26, 28, 41, 42
30-Sep-08	4.0	Ensure that policy, procedure and guidelines are implemented to enable the Department to monitor compliance of the following:	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	9, 15
	4.1	data cleansing and data governance	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	5, 13, 41
	4.2	information Asset Owners challenging data holdings	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	13
	4.3	the use of best practice	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	13, 14
	4.4	information Risk is addressed as a standing risk item on all Executive Boards and Audit Committees and assessed in Capability Reviews and in Office of Government Commerce	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	13, 18
	4.5	assurance processes analogous to those for Health and Safety are introduced for Information Risk.	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	13, 19

<b>E. Compliance - This is the process ensuring through Governance, Audit and Assurance that the Department continues to be compliant with current and future Legislation, Policy and Guidance.</b>			<b>Departmental Lead for Workstream</b>  <b>- DG Info</b>	
Date Due	#	Task	Resource	Burton Recommendations Supported
	4.6	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.	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	23
	4.7	initiatives making personal data accessible through secure links to central servers	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	25
	4.8	sharing personal data with third parties, including changes to mandated standard contractual clauses	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	6, 26
31-Mar-09	5	Ensure that policy, procedure and guidelines are implemented to enable the Department to monitor compliance of the following:	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	9, 26, 28, 29
	5.1	enforcement of security instructions by supervising officers	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	3, 8
	5.2	current and future system security procedures	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	8
	5.3	current and future requirements of the Data Protection Act	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	5
	5.4	all that require access to personal data are qualified at the relevant level	Info Advisor (Head DP and IA), DSSO, D Def Sy, TLBs, TFCEs	37

<b>F. Baseline and Improve - This is the process to establish the Departments current situation concerning Data Protection Act Compliance, Personal Data Holdings and Security of information and then improve it.</b>			<b>Departmental Lead for Workstream</b> <b>- DG Info</b>	
Date Due	#	Task	Resource	Burton Recommendations Supported
30-Jun-08	1.0	Instigate a census of all non laptop removable media across Defence by producing clear guidance and process which includes definitions, audit and reporting.	DG S&S, DG Info, TLBs, TFCEs	27
30-Sep-08	2.0	Review all relevant publications and amend where appropriate to ensure recording of non laptop removable media is mandated.	D Def Sy, DE&S	27
30-Sep-08	3.0	Instigate a census of all personal data held across Defence by producing clear guidance and process which includes definitions, audit and reporting (with specific reference to annual reporting against the SIC)	DG Info, TLBs, TFCEs	12
30-Sep-08	4.0	Instigate a review 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 by establishing legacy system gaps and taking remedial action	DG Info, DSSO	23, 26
31-Oct-08	5.0	Review all relevant publications and amend where appropriate to ensure recording of all holdings of personal data.	D Def Sy, DE&S, TLBs, TFCEs	12
15-Dec-08	6.0	Review existing best practice across Defence and OGDs to ensure that the Department identifies and acts promptly to correct mistakes; remains alert to identify, adapt and adopt good practice; and encourage and reward innovation	Info Access	15
15-Dec-08	7.0	Establish where changes to contractual clauses are required for existing systems to ensure the revised policy on sharing personal data with third parties.	DE&S	6, 26

<b>G. Technology - This workstream aims to ensure the department exploits information using both technology to the full, whilst ensuring all relevant risks are identified and mitigated.</b>			<b>Departmental Lead for Workstream</b> <b>- DG Info</b>	
Date Due	#	Task	Resource	Burton Recommendations Supported
31-Jul-08	1.0	Review options to procuring a simple, affordable solution to enable the safe, authorised, use of personal (privately owned, or MOD-provided) computers for limited Government tasks, on an individually licensed basis	Info Advisor and DES-ISS D Soln	36, 43
31-Jul-08	2.0	Review options to offer free and safe disposal of personal data devices. The review is to include for each option:	Info Advisor, DES-ISS D Soln	36, 44
		costs		
		risks and mitigation		
		consideration of balance of cost, risk and benefit		
30-Sep-08	3.0	Identify and accelerate support for initiatives making personal data accessible through secure links to central servers	Info Advisor, DES-ISS D Soln	25, 36
	4.0	Adption of best practise for data handling		15, 36
31-Oct-08	4.1	Review best practice from all sources (including OGDs, other Governments, private sector and the Information Commissioner) to enabled the Department to utilise technical solutions to ensure continued compliance with the Data Protection Act	Info Advisor, DES-ISS D Soln	
31-Mar-09	4.2	Adopt relevant best practice and incorporate into the Defence Information Strategy, and other relevant strategies, polices and guidelines	Info Advisor, Info Access, DES-ISS D Soln	

H. Accreditation - This workstream pulls together the accreditation related tasks.			Departmental Lead for Workstream - DGS&S	
Date Due	#	Task	Resource	Burton Recommendations Supported
31-Jul-08	1.0	Appoint a head of profession for Accreditation	DGS&S / DG Info	33
31-Oct-08	2.0	Establish policy on Personal Information Risk		34
	2.1	define a means of measuring risk exposure	DSSO/D Def Sy	
	2.2	declare the maximum level of acceptable risk (risk appetite) relating to personal information	DSSO/DG Info	
Ongoing	3.0	Ensure sufficient accreditation resource	2nd PUS, Head of Accreditation	35

<b>I. Governance - Confidence across the Department that information exploitation and protection is managed effectively in order to assure the confidentiality, integrity and availability of critical information and data.</b>			<b>Departmental Lead for Workstream</b> <b>- DG Info</b>	
Date Due	#	Task	Resource	Burton Recommendations Supported
30-Jun-08	1.0	Submit proposals on resourcing Action Plan to the Defence Board (two parts, in year and PR09)	Info Advisor	51
31-Jul-08	2.0	Embed Information Risk as a standing risk item for all Executive Boards and Audit Committees	D P&A	18
30-Sep-08	3.0	Mandate retention policy in Through Life Management Plans for new or unapproved projects (where appropriate) with responsibilities clearly defined between the relevant parties with reference to MOD's Data Protection Act record retention policy for personal data types.	DG Info, TLBs, TFCEs	6, 9, 23
30-Sep-08	4.0	Mandate governance processes within Through Life Management Plans (where practicable) for legacy programmes, and project approval and acceptance into service, taking account both of the legal requirements of the Data Protection Act and of security accreditation.	DG Info, TLBs, TFCEs	6, 9, 22, 23
30-Sep-08	5.0	Mandate governance processes within project approval and acceptance into service, taking account both of the legal requirements of the Data Protection Act and of security accreditation.	DG Info, TLBs, TFCEs	23
30-Sep-08	6.0	MOD to request Cabinet Office and Office of Government Commerce (OGC) to ensure Information Risk is formally assessed in Capability Reviews and in OGC Gateway Reviews	DG Info	20
31-Oct-08	7.0	Ensure that all relevant governance is developed, mandated, incorporated in Terms of Reference for supervising officers and maintained to support the detailed accountabilities for Data Protection across the Department (with specific focus on individual responsibility)	DG Info, TLBs, TFCEs	9
31-Oct-09	8.0	Ensure that all relevant governance is developed, mandated and maintained to support the role of Senior Information Risk Owner (with specific focus on communicating the terms of reference of the role across TLBs)	DG Info, TLBs, TFCEs	9, 19, 31
	9.0	Establish CIO and SIRO network across TLBs	DG Info, DG S&S, TLBs, TFCEs	19, 32

<b>I. Governance - Confidence across the Department that information exploitation and protection is managed effectively in order to assure the confidentiality, integrity and availability of critical information and data.</b>			<b>Departmental Lead for Workstream</b> <b>- DG Info</b>	
Date Due	#	Task	Resource	Burton Recommendations Supported
30-Sep-08	9.1	Review the options of formalising a network of TLB Chief Information Officers and Senior Information Risk Owners to provide coherent advice on the exploitation, security and assurance of information as a critical business asset.	MOD's 2-star IA Steering Group	
15-Dec-08	9.2	Consider and deliver the recommendations of the review of Chief Information Officer and Senior Information Risk Owners network across Defence	Defence Board, TLBs, TFCEs	
15-Dec-08	9.2	Provide a clear and accepted statement of Department CIO functional responsibilities that covers all areas of information risk and reinforce the authority of the MOD SIRO to act on behalf of the Defence Operating Board in respect of information risk	2nd PUS, VCDS	30, 31
31-Dec-08	10.0	Design and implement assurance processes analagous to those for Health and Safety for Information Risk	DG Info	19
31-Mar-09	11.0	Review legacy systems to enable (where practicable) mandation of a retention policy in Through Life Management Plans with responsibilities clearly defined between the relevant parties with reference to MOD's Data Protection Act record retention policy for personal data types.	DG Info, DG S&S, TLBs, TFCEs	6, 23
	12.0	Revised disciplinary framework		
31-Jul-08	12.1	Review existing policy to determine the current options available to deal with those who lose or compromise personal data, (military, civilian, government employee or contractor)	DCDS(Pers)/Personnel Director	38
31-Mar-09	12.2	Implement a disciplinary system, consistent with cabinet Office guidelines, that applies equitable censure to those that negligently or deliberately compromise personal information, while enabling the department to continue to learn and improve	DCDS(Pers)/Personnel Director	38

J. TAFMIS - This workstream is specific to issues raised about TAFMIS System.			Departmental Lead for Workstream - DG ART	
Date Due	#	Task	Resource	Burton Recommendations Supported
31-May-08	1.0	Review the Tri-Service business requirements against the Data Protection Act to enable TAFMIS to be compliant	ARTD, Front Line Commands	1
06-May-08	2.0	Design and implement a plan to bring TAFMIS into Data Protection Act compliance	ARTD, Info Access	7
13-Jun-08	3.0	Review the implementation plan with the Information Commissioner	Info Access	7, 21
16-Jun-08	4.0	Task EDS to implement plan	ARTD, EDS	7
31-Jul-08	5.0	ARTD and EDS senior leadership conduct a full review, provide a report and an action plan concerning the project management processes and procedures adopted within the TAFMIS project.	ARTD, EDS	4
30-Sep-08	6.0	Update the TAFMIS Through Life Management Plan to ensure continued compliance with the Data Protection Act and Information Management policy through relevant project governance processes	ARTD	4