Cabinet Office

Data Handling Procedures in Government: Final Report

June 2008

Making government work better

Contents

Foreword by Sir Gus O'Donnell

Effective use of information is absolutely central to the challenges facing the Government today – whether in improving health, tackling child poverty, or protecting the public from crime and terrorism. Those in public service need to keep that information secure, in order to build public confidence. This is essential to underpin greater data sharing to deliver personalised services and make us more effective.

Following the high profile loss of data by HM Revenue and Customs, the Prime Minister asked me to work with Departments and security experts to examine and improve data handling in Government.

This has involved intensive work across Departments and with their delivery bodies, which is summarised in this report.

Alongside the work in individual Departments, Government is improving the framework within which Departments manage information. This report sets out the action that is being taken to enhance consistency of protection, to get the right working culture in place, and to improve accountability and scrutiny of performance.

A lot has already been done, but there is more to do. This will inevitably be led largely in individual Departments, who are responsible for their own arrangements, but Cabinet Office will play its role in setting cross-Government standards and supporting Departments.

No organisation handling information can guarantee it will never experience losses. But people have a right to expect that their public services achieve and maintain high standards in this important area. Those involved in delivering those public services must work harder and be more effective to meet and exceed those expectations. Every loss or near miss must make us more determined. The action now underway will raise our game, but the task of improving information security will always be a continuing process.

GUS O'DONNELL

Summary

1. All modern organisations handle and manage information, including personal data, as part of their business. Central Government Departments are no exception. Better use of information can improve public services. It can make access more convenient, ensure people get all the services to which they are entitled, or allow services to be personalised. It helps to protect the public and fight crime including fraud.

2. People want improved services, but they also want their privacy protected. Therefore, Departments have to make sure that the right people get the information they need, whether on paper or by electronic means, while protecting information from others.

3. Achieving this is never simple. It is particularly challenging against a background of changing services and technology. Even before recent high profile losses, there was work underway across Government to get arrangements right. The loss of two discs by HM Revenue and Customs (HMRC) started an intensive process as all Departments re-examined their practices.

4. This work has been conducted in parallel with a set of independent reviews: the Poynter Review into the HMRC loss; the Burton Review into the loss of a Ministry of Defence laptop; and the Walport / Thomas review of data sharing, commissioned before the losses.

5. An Interim Report, published on 17 December 2007, summarised action taken across Government. That work has continued and broadened, and further progress is set out in Annex I. All Departments have placed restrictions on their use of electronic removable media. These are designed to ensure that personal data are only stored or accessed remotely in cases where it is absolutely necessary to do so. All Departments have started a broader process of cultural change, for example raising awareness among staff about handling sensitive data responsibly and securely, as well as their responsibilities under Departmental arrangements.

6. Looking forward, the challenges in this area are going to get harder rather than easier. The pace of technological change is quickening. The level and sophistication of external threats, such as e-crime, is increasing. Plans to improve public services will mean greater use of data within organisations and more data sharing. Meanwhile, existing challenges around secure handling of other information, such as paper, will continue. Sir David Omand is looking at the handling of highly classified documents to learn lessons from the recent incident. Sir Gus O'Donnell is looking at implementation of rules for the handling of documents across Government, taking account of Sir David's findings.

7. In response, as well as improving individual Departmental arrangements, Government needs to reform the overall arrangements within which Departments manage information. This report sets out how it is doing so, through:

- core measures to protect information, including personal data, across

Government, to enhance consistency of protection and transparency of that protection to others;

- a culture that properly values, protects and uses data, both in the planning and delivery of public services;
- stronger accountability mechanisms, recognising that the individual Department or agency is best placed to understand and address risks to their information, including personal data; and
- stronger scrutiny of performance, to build confidence and ensure that lessons are learned and shared.

8. The Interim Report set out initial directions of reform:

- using the existing line of accountability through Accounting Officers to Parliament as a way to improve information handling;
- setting clear common standards and procedures, including tightening procedures for data stored overseas;
- increasing visibility of performance, with Departments publishing material in their annual reports, and a report on the issue as a whole to Parliament; and
- commitment by Government to provide the Information Commissioner with new powers to conduct "spot checks", and to introduce new sanctions under the Data Protection Act for the most serious breaches of its principles.

9. This report describes how Government has now put in place new measures to protect information, to apply across central Government. No organisation can guarantee it will never lose data, and the Government is no exception. But the actions in place:

- introduce obligatory use of protective measures (such as encryption and penetration testing) and controls (for example on use of mobile devices or on access to records). These will protect all personal data, while recognising that some data require a greater degree of protection than others;
- reinforce efforts to ensure that civil service working culture supports the proper use of information. This applies both at the planning stage through use of Privacy Impact Assessments and when services are being delivered. There will be mandatory training for those with access to protected personal information or involved in managing it, alongside new action to make clear that any failure to apply protective measures is a serious matter potentially leading to dismissal;
- standardise and enhance the processes by which Departments understand and manage their information risk, setting out the responsibilities for key individuals in doing so; and
- further enhance transparency of arrangements, through use of information charters, and greater publication of information on particular information assets and their use.

10. The new actions in this report supplement and augment material provided to Departments in other ways, including through the Manual of Protective Security and the Civil Service Management Code. They set out minimum rules, in that individual Departments and agencies will continue to assess their own risk and often put in place a higher level of protection. The Government's guiding principle is that the protections outlined in this report, or their equivalent, should be in place and effective, no matter how information is held and processed for UK Government purposes. The same standards will be applied by contractors. Work is underway to develop equivalent material for the wider public sector.

11. Compliance will be assessed on an annual basis, and underpin the summary material in the Statement on Internal Control, and be the subject of peer review, through capability reviews and as requested by particular Departments. External scrutiny of performance and capability will be provided through:

- National Audit Office scrutiny of the Statement on Internal Control, using their knowledge of the organisation in question;
- spot checks by the Information Commissioner; and
- targeted intervention by Departments and CESG, the National Technical Authority for Information Assurance in GCHQ, to assess counterparts' systems and protections.

12. The Cabinet Office's responsibility is to review and update cross-Government standards in the future to accommodate lessons learned and new developments. Cabinet Office is adapting its resources to the new way of working set out in this report. Furthermore, to support implementation, cross-Government structures are being streamlined, with a particular emphasis on provision of support in areas like training and professional development, and on understanding cross-Government risks and what those mean for the overall Government framework.

13. The changes set out in this document are significant and, although much has already been done, there remains much to do. Progress will be overseen by the Cabinet Committee on Personal Data Security, chaired by Paul Murphy, the Secretary of State for Wales. Departments will report on progress made in their annual reporting. Cabinet Office will follow these with the first annual reporting on the issue as a whole following the end of 2008/09.

Section 1: Scene-setting

This work was commissioned by the Prime Minister following high profile data losses in 2007. The aim was to assess and improve procedures for the use and storage of data in Government. It has been conducted alongside specific work into losses in HMRC and the Ministry of Defence, as well as more general work on data sharing being conducted by Richard Thomas and Dr Mark Walport.

Public service delivery relies on the right information being available to the right people. Better use of information can mean better services, through personalisation and by ensuring that people get all the services to which they are entitled. It helps to protect the public and fight crime. But services have to be planned and delivered while maintaining individual privacy.

The Data Protection Act and Human Rights Act provide the legal framework to safeguard privacy. Departments and their agencies are best placed to manage their own information, and are responsible for doing so. Cabinet Office, HM Treasury and the Ministry of Justice set the framework within which they manage information, and, with others, provide assistance. Government arrangements in this area have been the subject of on-going work, and action was underway to improve them before recent losses.

Good practice in managing information may be drawn from the public and private sectors. Technical and process measures need to be taken to minimise the scope for error or malicious action. Organisations need to achieve a culture that underpins the safe use of information, both when planning business and operating it. Clear accountability is vital, particularly at senior levels, to ensure that risks to information are considered from the start. Because no information handling system provides total protection, performance needs to be monitored and lessons learned on an ongoing basis.

Managing information risk in the public sector is likely to become harder in the future rather than easier. Technology and external threats both continue to change quickly, while the use of information in the public sector is likely to increase as services are improved.

A great deal of work has been done in Departments to improve data handling arrangements, and more is planned. But there must be continued vigilance to ensure the highest possible standard of information security.

Report scope and relationship to other work

1.1. On 21 November, following the high-profile data loss from HM Revenue and Customs (HMRC) the Prime Minister announced that he had asked the Cabinet Secretary, with the advice of security experts, to work with Departments to ensure that they and their agencies check their procedures for the storage and use of data.

1.2. The terms of reference for the work were to examine:

- the procedures in Departments and agencies for the protection of data;
- their consistency with current Government-wide policies and standards;
- the arrangements for ensuring that procedures are being fully and properly implemented; and

  to make recommendations on improvements that should be made.

1.3. There are close links between personal data handling and information handling. The processes involved in successful management are similar. They involve understanding what is held, what the risks are to that information, and then mitigating them. As a result, while this work has focused on personal data, its conclusions are relevant to information more generally, whether held in paper or electronic form. In addition, Sir David Omand is looking at the handling of highly classified documents to learn lessons from the recent incident. Sir Gus O'Donnell is looking at implementation of rules for the handling of documents across Government, taking account of Sir David's findings.

1.4. This report examines information used by central government bodies and contractors to deliver central government objectives. It has not addressed data storage and use in the private sector, other than when they work as contractors, or by public sector bodies in other countries.

1.5. Within this focus, the work has concentrated on central Government bodies. Local government and other independent public sector organisations also play crucial roles in the delivery of public services. The aim has to be for consistent standards to be applied. The position for the wider public sector is considered in Section 3.

1.6. In examining data handling and use, the work considers both use of data within a given organisation and use when data are shared, but does not seek to explore issues specifically around data sharing. The work considers how data can be kept safe and how it should be handled, rather than whether sharing of particular data in a particular way is desirable. A review of data sharing in the UK public and private sectors is currently taking place, led by Richard Thomas, the Information Commissioner and Dr Mark Walport, Director of the Wellcome Trust. This will report shortly.

1.7. The work has been conducted alongside other detailed examinations of arrangements in specific Departments. The Poynter Review has examined the circumstances around the loss of data in HMRC[1], and the Burton Review has examined the circumstances around the loss of a laptop in the Ministry of Defence[2].

1.8. An interim report for this review was published on 17 December 2007. That report briefly summarised action being taken in each Department to examine and assess their arrangements for the handling of data. It also set out some initial reforms to the overall framework within which Departments manage their information, notably:

- building on the existing line of accountability through Accounting Officers to Parliament to improve the handling of information risk. Information assurance would be covered explicitly in annual Statements on Internal Control;
- setting clear common standards and procedures, including tightening procedures for data stored overseas;
- increasing visibility through Departments publishing material in their annual reports, and a report on the issue as a

[1] www.hm-treasury.gov.uk/independent_reviews/poynter_review/poynter_review_index.cfm

[2] www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080207/wmstext/80207m0001.htm

whole to Parliament; and

- greater scrutiny through "spot checks" conducted by the Information Commissioner, and the introduction of new sanctions under the Data Protection Act for the most serious breaches of its principles.

Government policy and use of information

1.9. The public sector depends on information to deliver public services, such as: paying benefits; delivering the National Heath Service; and managing the driving licence system. Organisations across the public sector collect, use and store a wide range of personal information, such as income, date of birth and health records, in order to carry out their work. Information is used to check identity and confirm eligibility and to detect and prevent fraud.

1.10. If Government is to deliver joined up services focused on the customer, it needs to know with whom it is dealing. This relies on information being available about the people being served. In the most extreme cases, failure to make information available can lead to serious harm to individuals, for example by failing to prevent crime. It can mean that vulnerable groups in society cannot be provided with the support they need.

1.11. As information and communications technology (ICT) systems become capable of storing and using more information faster, Government has the opportunity to design and develop better services using information from different sources. The difficulty and inconvenience caused to people trying to negotiate different parts of the public sector can be reduced considerably. The Government has set out a vision to ensure that information will be shared to expand opportunities for the most disadvantaged, fight crime and provide better public services for citizens and business, and in other instances where it is in the public interest.[3]

1.12. Some of the benefits in this area are already being realised. In the pension service, pensions and other benefits can now be obtained in one phone call, rather than filling in large amounts of paperwork.

1.13. While sharing information can offer new ways of delivering public services, it has to be done in a way that preserves individual privacy. The Data Protection Act (1998) and Human Rights Act (1998) set out the legal basis for the handling of information and the right of the individual to privacy. The need to use information to maintain security for society may be balanced, in some cases, against the rights of the individual, for example by sharing criminal records. The Freedom of Information Act (2000) set out the public 'right to know' in relation to public bodies.

1.14. The policy aim of the legal framework is to provide individuals with the assurance that their information will be protected and used only for legitimate purposes. As such, it supports the Government's intention to increase legitimate use of information, to increase public benefit and public protection. It is clear that there are sometimes difficult lines to draw about what is or is not a legitimate use of information. These are complex questions that are being explored in the Walport / Thomas review and are not further examined here.

1.15. Government has already introduced a new monetary penalty in the Data Protection Act (sections 55A to 55E). These ensure that data controllers who do not take reasonable steps to avoid the most serious breaches of Data Protection Act principles may be subject to a fine as well as to an enforcement notice.

1.16. There are also instances in which people deliberately and recklessly misuse personal data. The Information Commissioner has highlighted a lucrative and illegal trade in personal data. The Government takes this matter very seriously, and has amended the Data Protection Act to provide an order-making power to increase the maximum penalty for such offences. The maximum that could be specified in such an order would be two years imprisonment. This is intended as a strong signal that such action will not be tolerated.

1.17. Where Government holds or uses

[3] http://www.foi.gov.uk/sharing/information-sharing.pdf

personal information, it must act as the custodian of that data and retain and build public confidence that information is held securely. This is particularly true where the law requires that Government be given information, such as in the case of financial information for tax records. Loss of public trust will mean that public services cannot be delivered efficiently or effectively. At the same time, the failure to make the right information available at the right time can have an adverse impact on public services.

1.18. Management of information is integral to the management of public services. Departments and their agencies are best placed to manage their own information and are responsible for its security. That is because they understand best what information they hold, how it has to be used, and the consequences of the risks they face.

1.19. Departments and their agencies exercise that responsibility within a number of frameworks:

- the law (discussed above) for which the Ministry of Justice is responsible;
- a strategic information assurance and security framework set by the Cabinet Office for Departments to implement;
- corporate governance and accountability requirements, promulgated by HM Treasury; and
- the Civil Service Management Code, promulgated by the Cabinet Office.

1.20. The Information Commissioner plays a statutory role in policing compliance with the Data Protection Act, and provides advice on relevant legislation and good practice.

1.21. In addition, there is a range of policy interests that are relevant to information use. Every Department constantly examines its services to seek to improve them, and many of the changes result in changes of information use.

1.22. In planning arrangements, Departments seek to maximise the impact of their activity while managing risks. As a result, they adopt a range of delivery mechanisms. Some services are delivered directly, some by arm's length or independent public bodies, and some by contractors.

1.23. When this work was commissioned in November 2007, there was already work underway to improve arrangements for data handling in Government. The Cabinet Office had commissioned an independent review to examine the Government's capacity to achieve information assurance in the era of Transformational Government. This work informed a refreshed National Information Assurance Strategy, published in June 2007. That Strategy set out an approach for improving information risk management through increased professionalisation and awareness raising, availability of information assurance products and services, and compliance and adoption of standards.[4]

Good practice

1.24. The challenges Government faces regarding information risk management are not unique to the UK or to the public sector. This section summarises good practice. The material is drawn from material made available by Departments, interviews with business, and input from external experts.

Specific measures

1.25. Organisations apply similar cycles of assessing their information, understanding the risks relating to that information, and planning mitigating action. This mitigation is then put in place and monitored.

> Company A adopts a risk-based approach to its staff, with regular vetting procedures for employees in accordance with their level of exposure and access to sensitive personal data. Staff are by default provided with minimum user access rights. Line managers are accountable for system access rights within their team and are required to evaluate the appropriate level of access rights for each role in their team, put forward a business case for additional access, and review and report on those access rights on a regular basis.

1.26. Strong common standards and controls are needed to control access to IT infrastructure. Business managers are

[4] www.cabinetoffice.gov.uk/csia

required to evaluate and declare appropriate access rights for each role in their areas and review those rights regularly. New members of staff are provided with access rights only on successful completion of training and minimum access rights are issued as a default.

1.27. Access to raw data are kept to a minimum in business areas with potential access to a high volume of data such as call centres, or areas with high staff turnover. Every information asset is classified and risk assessed by the relevant data owner.

1.28. Private sector organisations aim to use contractual terms to clarify ownership of data, allow regular due diligence checks, and preserve continuity, even where there is a changeover of contractors. They may assess contractors upfront to ensure they can meet the organisation's standards.

Culture

1.29. Strong organisations seek to foster a culture of individual accountability throughout the organisation, with targeted, relevant, role-based training to ensure that employees have a clear understanding of how to use and share information securely. At the same time as recognising the importance of cultural change, many commentators highlighted the difficulty of achieving it and the time taken to do so.

Company B has initiated a concerted recruitment drive for information security staff who are able to communicate and present clearly how security risks affect the business, in the context of the organisation, and provide clear, relevant and practical guidance for senior management and staff. This is considered to be as important a skill as demonstrating technical expertise.

1.30. Information is seen as a key corporate asset and employees consider themselves 'trusted stewards' of sensitive data with an obligation to protect it. Data are valued throughout its lifecycle to ensure the maintenance of accurate and current records, with clear review, retention and disposal policies in line with relevant legal and regulatory frameworks.

1.31. Staff awareness and education programmes are often supported by regular, centrally monitored testing to assess employees' understanding and ability. When information security skills are included in the performance management framework they are underpinned by disciplinary measures. A learning system is needed, where people avoid mistakes where they can, but admit errors where they are made. This encourages continuous improvement by learning from mistakes, and enables the business to be honest with its customers about possible errors with their data.

Company C has a bespoke e-learning training programme, tailored to role, which staff are required to complete on an annual basis. At the end of the training they complete a short test online, the results of which are sent to their line manager. New modules are rolled out in response to specific information security threats which staff are directed to when they log on.

1.32. However, it is important to set clear expectations about what constitutes an offence for which employees may be disciplined. Several interviewees commented that the rare occasions where an individual had been fired for misconduct, such as looking up the records of neighbours, served as strong deterrents.

Accountability

1.33. Senior level ownership of information risk is a key factor in success. Senior leadership demonstrates the importance of the issue and is critical in obtaining resource. A simple governance structure, with clear lines of ownership, is essential. Well defined roles and responsibilities are needed to follow up identified information security threats and managing incidents. Internal audit can play an important role in examining and assuring actions taken by others.

Scrutiny and transparency

1.34. Organisations work with the Information Commissioner's Office to ensure compliance with the legal and regulatory framework, and maintain open communication about the data they hold, how it is used, and consumers' rights with respect to the use of their information. Providing clear guidance on who to contact in the event of a query or complaint is key to maintaining customers' trust.

Future challenges

1.35. Looking forward, the challenges of ensuring information security are likely to increase. This is as a result of changing technology and external threat. The greater use of information to improve services will add complexity to the problem.

1.36. The pace of technological change is likely to continue to accelerate. New technology to protect data in storage can be used to enhance security, but at the same time the pace of development, such as on wireless technology, adds complexity by creating new opportunities for exploitation.

1.37. Risks posed by deliberate action will remain significant. The threat from hacking and malicious software remains ever present and is becoming increasingly sophisticated.

1.38. Organised crime increasingly exploits the growth of the Internet, particularly in commerce and finance, to develop new crimes and transform traditional ones. The rapid growth of the Internet has resulted in the development of a criminal economy dedicated to the compromise, trade and exploitation of private data. The personal data held by Government are valuable to organised crime and, as a result are at risk from attack.

1.39. A number of countries continue to devote considerable time and energy seeking to obtain information on civilian and military projects in the UK, and political and economic intelligence. This results in attempts to penetrate Government information systems.

1.40. Meanwhile, as part of improving public services, more use will be made of information. This will mean greater connectivity and, therefore, new challenges to ensure that supporting controls and culture are consistent throughout the public sector. At the same time the Government must maintain its focus on protecting the large amount of information that continues to be handled in paper form.

1.41. The main responsibility for understanding and managing information risk should be discharged by the individual Department or agency. Managing information is integral to managing the business and should be handled accordingly.

1.42. Departments and their agencies have checked their procedures for the storage and use of data and their consistency with current cross-Government policies and standards, as well as arrangements for ensuring that procedures are being fully and properly implemented. An update on this work was provided through the Interim Report. A further update is provided in Annex I.

1.43. A wide range of work has taken place across Government. Many of the larger Departments who handle large volumes of personal data have initiated specific reviews into the management and handling of information throughout their organisation. Some have started designing and rolling out training and awareness programs for staff using a range of delivery methods. All Departments have been working with their delivery partners to roll out encryption for the laptops holding personal data where it was not previously in place.

1.44. In parallel, Government has developed its understanding of the need for reform to the overall standards within which Departments operate, building on the recommendations in the Interim Report.

1.45. It is clear that there will be demand for greater information sharing between public bodies, driven by the desire to improve public services or fight crime. Responding to this demand is likely to mean that common standards will become increasingly important.

1.46. Since the Manual of Protective Security[5] and other key documents are protectively marked, they are not published. This makes it difficult for others to understand and assess the approaches being adopted. While it will never be right to make the Government's security arrangements completely public, greater visibility can play a useful role in the public debate and in helping suppliers and partners anticipate key requirements that Departments will be looking to meet.

1.47. Government needs to recognise and

[5] The MPS is under revision and will be promulgated later this year as the Security Policy Framework in a more accessible form

respond to the need to nurture a culture that values, protects and uses information. UK public servants who inevitably handle information must understand the importance of privacy. However, there is a risk that service and technology changes may move faster than culture can adapt.

1.48. Following recent losses, Departments are working to test and where necessary to enhance their arrangements. Continued focus on the issue will be essential, particularly in light of future challenges. This means it makes sense to strengthen the accountability mechanisms for Departments, and scrutiny of their performance.

1.49. Government is therefore enhancing its arrangements through:

- core measures to protect information, including personal data, in place across Government;
- a culture that properly values, protects and uses data;
- stronger accountability mechanisms; and
- stronger scrutiny of performance.

1.50. Actions to achieve these aims are set out in the following section.

Section 2: Better data handling

This section sets out how the Government is improving data handling, to achieve:

- core measures to protect information, including personal data, in place across Government, to enhance consistency of protection and transparency of that protection to others;
- a culture that properly values, protects and uses data, both in the planning and delivery of public services;
- stronger accountability mechanisms for Departments. The individual Department or agency is best placed to understand and address risks to their information, including personal data; and
- stronger scrutiny of performance, to build confidence and ensure that lessons are learned and shared.

Each topic is covered below.

Core measures to protect information

Departments are already provided with a wealth of security policy advice, guidance and information, notably in the Manual of Protective Security and the Civil Service Management Code. While these remain important parts of the regime, they need to be supplemented with a shorter set of core minimum requirements that are applied across the board. Departments will still determine the level of protection that is applied in particular circumstances, and will often go further than the minimum. But the new requirements in effect introduce a common level that they must meet.

The measures have been developed to reflect the wide range of activity by Departments and their delivery bodies. Some of these handle huge volumes of highly sensitive information, while others handle much less. The approach and material has been developed with the input and support of the Information Commissioner, and will be updated in the future in the light of experience.

Specific elements of the package relating to the transfer of data include:

- specifying personal data benefiting from higher levels of protection;
- where possible, not transferring such information, but accessing it on its home system or remotely via a secure channel;
- where transfer must occur, doing this through secure electronic transfer, so that discs are phased out where possible; and
- where data have to be put onto removable media such as discs or laptops, minimising the information transferred, and using encryption.

Departments are putting in place new controls to limit user rights to transfer data to removable media such as discs and to check the use of those rights.

In addition, new core requirements cover:

- securing disposal for paper or electronic records;
- using independent penetration testing to test Departmental systems;
- controls on access to information systems and logging and monitoring of use; and
- increasing the use of the "accreditation" process, developed to provide assurance for systems holding national security information, for systems holding personal data.

2.1. The Data Protection Act defines "personal data" and "sensitive personal data". While the Government will continue to process all personal data in accordance with Data Protection Act requirements, neither is suitable for an administrative definition of information attracting certain technical protection. While all personal information is of value, the right technical level of protection varies significantly within the "personal data" category. "Sensitive personal data" is so specific as to exclude important aspects of information that require high levels of protection. As a result, this work has, with input from the Information Commissioner, specified an intermediate category of information, referred to as "protected personal information".

2.2. This definition relates to any material that links an identifiable individual with information that, if released, would put them at significant risk of harm or distress, or alternatively any source of information relating to 1000 or more individuals that is not in the public domain, even if the information about an individual is not considered likely to cause harm or distress. As in other areas, this is a minimum baseline. Departments will often wish to apply protection to smaller data sets depending on their risk assessment and the context in which information is kept.

2.3. Wherever possible, Government should keep such protected data within secure premises and systems. This means minimising the storage of, and, access to personal data on removable media, such as laptops, computer discs and memory sticks which may be lost or stolen. A hierarchy of options has been established with the accessing of data on secure systems in secure premises as the best method of handling and accessing personal data. Where transfer must occur, Departments must consider whether it is possible to provide secure remote access so that data can be viewed without being permanently stored elsewhere.

2.4. Where the use of removable media is unavoidable, encryption will be used and the information transferred will be the minimum necessary to achieve the business purpose. There will remain some situations where encryption cannot be applied consistent with the business purpose – for example for back-up tapes that need to be accessible immediately – such material will be afforded physical protection using similar risk assessment processes as for large amounts of public money or precious objects. This is not an attempt to assign a monetary value to information, which can be complex and may be misleading, but to ensure appropriate secure arrangements for storage and transportation of what are key assets. Both paper and electronic records will be subject to secure disposal.

2.5. To test protections of IT systems against external attack, Departments whose delivery chain involves the handling of information relating to 100,000 or more identifiable individuals will use independent experts to conduct penetration testing.

2.6. To protect against misuse of information, access rights will be minimised, and arrangements put in place to log use of electronically held personal information. Both will be scrutinised by senior individuals.

2.7. Departments will make greater use of the accreditation process for IT systems. This process was developed to provide assurance to the senior business owners of systems holding national security information, and involves an expert assessor

examining plans to ensure that information risk has been adequately addressed. New ICT systems containing protected information will be accredited to the Government standard and their accreditation status will be maintained throughout the life of the system.

2.8. The measures developed apply to situations when data are held or used within Government. High levels of data security are also important in citizen or industry-facing activity. Such activity can include both sending and receiving information, which can be sensitive. Departments cannot take responsibility for how others send information to them, although they can encourage good practice, and potentially refuse to accept material that is not handled safely. However, individual citizens may prefer to send or receive information in a way that is less secure, if it makes a service more convenient. Departments will seek to apply the same levels of protection when dealing with those outside Government as have been developed for use inside Government, while recognising that there may be a case to set other standards or make other arrangements. Where different standards are set, they will be clearly explained, along with alternative service routes.

Culture

High levels of data security must be underpinned by a culture that values, protects and uses information. This culture is important both when services are being planned and when they are being delivered.

Government is reinforcing its efforts to ensure that the right culture is in place. This has to be led from the top of Departments, and include all those involved in the management of and access to personal data. As in other areas, individual Departments are responsible for their own data security, and will need to lead the work, tailoring it to their circumstances. Departments will need to understand and actively manage any day-to-day operational processes that may, wrongly, lead staff to cut corners and expose information, in whatever form, to unacceptable risk.

Government should regard any data loss as a cause for concern, and take immediate action to improve matters for the future. When problems occur, however, the culture has to be one in which losses are identified and learned from. This should apply both to actual problems and “near misses”. This is vital if Government is to avoid making the same mistakes, as well as allowing Government to be open with individuals who may be affected by problems.

All Departments will take the following action:

- introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start, and those planning services are clear about their aims. Similarly, information risk management will be considered as part of the Government’s “Gateway™” reviews that monitor progress of the most important projects;
- roll out a basic level of mandatory training to all data users and those involved in managing personal data, to be completed on appointment and annually;
- put in place processes by which individuals can bring concerns to the attention of senior management, anonymously if necessary; and

- amend HR processes where necessary to make clear that failing to apply controls in handling personal data could amount to gross misconduct.

Action will be taken by Cabinet Office with others to increase the professional qualifications of those involved in information assurance.

2.9. Most of those contributing to this work have stressed the importance of the right culture to underpin data security, if information risk is to be understood and efficiently handled in day-to-day operations as part of normal business. Any operational process that may, wrongly, lead staff to cut corners and thus expose information, in whatever form, to unacceptable risk must be identified and actively managed. Departments should put in place plans to lead and foster a culture that values, protects and uses information for the public good, and monitor progress, as a minimum through standardised civil service-wide questions in their people surveys.

2.10. The culture of an organisation affects its ability to protect its information in many ways. It affects the attitude to collecting information in the first place, and how systems are developed to do that. In recognition that collecting any sort of information potentially brings risk with it, good practice requires that privacy protection and data security are built into plans at the earliest stages.

2.11. The Information Commissioner has made a powerful case for Government to adopt Privacy Impact Assessments. These are structured assessments of a project's potential impact on privacy, carried out at an early stage.[6] They enable organisations to anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions. Risks can be managed through the gathering and sharing of information with stakeholders. Systems can be designed to avoid unnecessary privacy intrusion, and features can be built in from the outset that reduce any impact on privacy. The Privacy Impact Assessment adopts a risk management process approach, periodic reports from which (Privacy Impact Assessment Reports) may be published or distributed to stakeholders. The Government has accepted their value and they will be used in all Departments. Future "Gateway ™" reviews of ICT projects will check that they have been carried out as an integral part of the risk management assessment.

2.12. The OGC Gateway™ process is designed to examine the progress and likelihood of successful delivery of programmes and projects. Its use is mandatory in central Government for procurement, IT enabled and construction projects. An examination of project risk is an integral part of the Gateway™ Process, which will include information risk as well as privacy.

2.13. The operating culture of an organisation is also important. If staff understand the value of information and the potential threats to it, management and staff will find ways to deliver the services expected of them without exposing information, in whatever form, to unacceptable risk. They will keep alert to attempts by outsiders to gain illegitimate access to it, and can be an important source of ways to improve protections and arrangements.

2.14. Government will roll out at least a minimum level of information risk awareness training to all those with access to protected personal data. This will supplement training already in place to make staff and contractors aware of their responsibilities for safeguarding and handling information in accordance with the Manual of Protective Security and the Civil Service Management Code. Such training will, where possible, take the form of short, e-learning products including tests for understanding, and will be applied on appointment and annually.

2.15. To support a managerial culture that understands the importance of information and deals actively with risks to it, Government will roll out at least a minimum level of information management training to

[6] http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/foreword.html

all Information Asset Owners (see below under Accountability), on appointment and annually, and strategic information management training to Accounting Officers, Senior Information Risk Owners, and members of audit committees.

2.16. Cabinet Office will provide a minimum specification for this training, and seek views from Departments as to whether they would wish to use a standardised training product. The aim should be to develop training material that can be externally accredited and transferred between organisations, and integrate similar material into relevant courses run by external bodies.

2.17. Government needs to increase the professional qualifications of staff involved in information assurance work. The National Information Assurance Strategy set out the need to increase professional capacity. Cabinet Office will take this forward, working with others. The right links will need to be made with the closely related areas of IT and knowledge and information management, and with the work to develop professional capacity and capability in those areas.

2.18. HR processes in Departments will be amended where necessary to make clear that failing to apply controls in handling sensitive data is a serious matter, and could amount to gross misconduct.

Stronger accountability

The onus has to remain on Departments to plan and secure their own information. This is because protection and use of data are part and parcel of their business, and they are best placed to understand requirements and manage risks. The best mechanism to ensure that this happens is the chain of command from the Accounting Officer, who is ultimately responsible for having the appropriate controls in place in their Department.

However, more can and should be done to increase accountability, in particular to standardise and enhance the processes by which Departments understand and manage their information risk, setting out the responsibilities for key individuals in doing so. Departments are required to establish:

- a process by which information assets are identified and allocated to a responsible owner; and
- an annual assessment process to support the Accounting Officer's judgement for the Statement on Internal Control.

Simplified cross-Government structures will support this process, with Cabinet Office maintaining and updating the cross-Government requirements.

Responsibility in Departments

2.19. Most Government Departments are large, complex organisations. They can undertake very different tasks. In doing so, they draw on a wide range of expertise, including experts in knowledge management, ICT, information management, security and others. They approach their tasks in different ways. Different roles may be legitimately combined in different circumstances, so a single solution cannot be applied. But roles on information management and risk must be sufficiently standardised to drive responsibility and accountability. Similarly, it is necessary to balance the need to avoid unnecessary bureaucracy with the need to ensure that important decisions are considered, recorded and implemented.

2.20. Government has developed a set of specific actions to achieve these aims.

These build on good practice and international standards, and on established roles of the Accounting Officer and the Senior Information Risk Owner, who is a board level executive with particular responsibility for information risk. They are tailored to the circumstances of the UK central Government. Many Departments will, as now, work towards or achieve external ISO accreditation for some or all of their information systems, but independent input to this work suggested that systematic external accreditation would absorb effort that would be better used in a more targeted way.

2.21. Departments are now standardising and enhancing the processes by which they understand and manage their information risk, including by:

- defining their information risk policy, which says how information risk will be managed within the Department and by their delivery partners and how effectiveness will be assessed;
- identifying information assets, and giving senior individuals involved in running relevant businesses (Information Asset Owners - IAOs) clear responsibility for each in defined ways;
- assessing risks to the confidentiality, integrity and availability of information in their delivery chain at least quarterly, and putting in place responses to manage those risks as necessary; and
- specifying an annual process of assessment to provide an evidence base to support the judgement of the Accounting Officer, including written input from Information Asset Owners and the Senior Information Risk Owner.

2.22. The role of the Information Asset Owner is to understand what information is held and in what form, how it is added and removed, who has access, and why. They approve the level and extent of transfer of data to removable media, such as laptops, ensuring that it is the minimum necessary to conduct the business, and that it is properly protected. They ensure that access rights to IT systems are limited to the minimum needed, and that usage of information is monitored. Importantly, they are tasked with ensuring that best use is made of information, and receive and respond to requests from others for access to information.

2.23. In addition to these named roles, Departments will need to ensure that they have the right mix of professional advice and support, covering both risk and information issues specifically.

2.24. Putting in place these new arrangements represents a significant undertaking for most Departments, but they have committed to do so, and implementation has commenced. Departments' first full annual assessments will be completed for the year 2008/09 and reflected in Statements on Internal Control, the standard way of bringing risk management within an organised structure for reporting and internal use.

2.25. As Government bodies share more information, whether to improve services or to protect the public, they are increasingly developing information systems that reflect the interests of several different organisations. Contrary to some public perception, such systems may not be all-encompassing databases, but mechanisms to link together and make better specific use of information that is held separately.

2.26. Clear accountability and responsibility are crucial for effective operation of systems that cross Departmental boundaries, just as they are for systems operating within Departments. Government is learning to adapt established approaches to these new situations, in particular:

- ensuring that every system has a single Senior Responsible Owner[7] (SRO). The SRO is responsible for the business case and ensuring that the system achieves its aims. The SRO does this through management of the associated risks by ensuring that the right controls and protections are built in and monitored so that participating organisations can use it with confidence;

[7] The OGC definition of the SRO may be found at: http://www.ogc.gov.uk/User_roles_in_the_toolkit_senior_responsible_owner.asp

- ensuring that information enters a system with the agreement of the owning Department, in effect that the controls provide sufficient protection; and
- the SRO, working with the IAO ensures that there is an individual responsible for the continued integrity of datasets, maintaining and enforcing application of policies and standards applicable to the system and scrutinising the system, remaining alert, for example, to the creation of new dataset combinations which raise new system challenges and, potentially, privacy concerns.

2.27. Cabinet Office will continue to set the overall standards for information assurance in Government, taking account of the need both for security and for knowledge and information management to assist in the delivery of public services. Responsibility for specific implementation of the regime in each Department lies within that Department. Cabinet Office will support the strengthened regime set out in this report by:

- setting the cross-Government mandatory standards. These will need to be updated in the light of experience, and of progress in Departments in implementation. Crucially they will need to continue to be informed by business experts, technical experts, and independent input from others;
- provision of practical support for implementation in Departments, for example developing and providing services of common interest, where it may be more efficient for Government to develop a single solution to a shared problem than to develop many different approaches. This will require the acceleration of the work to improve support to Departments foreseen in the National Information Assurance Strategy. Cabinet Office will provide support where it is best placed to do so, and co-ordinate others where that is a more effective approach;
- preparation of the annual report on information risk as a whole, including on the level of "common good" spending on information assurance needed for Government and specific policy issues as they arise.

2.28. In common with other policy areas, Cabinet Office can play a role in identifying and resolving issues that cannot be easily resolved between individual Departments. Experience shows that specific data sharing proposals can fall into this category. The network of Information Asset Owners provides a mechanism to identify such issues.

2.29. In addition, cross-Government functions will be reformed, in order to:

- understand information risk better across Government and, in particular, provide a central facility for sharing risk information. Cabinet Office will receive the annual assessments from Departments, and use those to develop a cross-Government view of the risks being faced by Departments, to inform work on updating the common standards, or other action; and
- simplify the complex array of groups active in the information risk area, which have developed over time in response to particular needs, but which can now be usefully consolidated.

2.30. Cabinet Office is committed to take forward these tasks, working with others. Cabinet Office is adapting its resources to the new ways of working set out in this report.

2.31. During the preparation of this report, the team benefited from input from a range of individuals and bodies, including industry and academia (see Annex III). The Government will maintain strong levels of engagement, in addition to the regular dialogue with potential suppliers that is already in place and seeking advice on best practice from independent experts.

2.32. Implementation of the action underway as a result of this report will be taken forward through a cross-Departmental programme, supported by a committee of senior officials. Collective Ministerial overview and approval of the report on information risk across Government will be provided by the Cabinet Sub-Committee on Personal Data Security, chaired by Paul Murphy, Secretary of State for Wales.

Stronger scrutiny

In publishing the Interim Report, the Government committed to enhanced transparency of actions. Departments will cover information assurance in their annual reports, and the Government will report annually to Parliament on information security as a whole. This commitment will now be reinforced through:

- the publication of Information Charters by all Departments. These set out the standards that people can expect from public bodies that request or hold their personal information, how they can get access to their personal data and what they can do if they do not think that these standards are being met;
- consideration by Departments of publication of material on specific information assets held, such as what information is contained and how it is used. This is to be considered with a presumption of openness, while recognising that there will always be some information and some uses of it (for example in the national security and law enforcement arenas) where transparency must rightly be limited; and
- publication by Cabinet Office of the new requirements on Departments[8].

Performance and capability will be monitored by a combination of specific controls, as well as by building information risk into existing mechanisms:

- reference to information assurance in the Statement on Internal Controls, which is subject to scrutiny by the National Audit Office (NAO), based upon their knowledge of the organisation in question;
- spot checks conducted by the Information Commissioner, or other more formal action, including application of existing sanctions of the Data Protection Act or new sanctions when they are in place; and
- inclusion of information risk issues in Whitehall "capability reviews".

In addition, given the greater connectedness of Departmental systems, Departments will be able to request on a peer basis additional assurance about their counterparts' systems and protections. Within this, CESG, the National Technical Authority for Information Assurance, will be an active and important source of expert scrutiny of performance.

[8] http://www.cabinetoffice.gov.uk/csia

2.33. Following the requirements in this report, Departments will produce a range of internal material including:

- the information risk policy;
- quarterly risk assessments, including actions planned as a result;
- accreditation records; and
- an annual review against requirements, supported by evidence-based assessments from the SIRO and IAOs.

2.34. Together, these provide a clear audit trail between the detailed work to manage information risk and the judgement of the Accounting Officer in their Statement on Internal Control. This audit trail will be an important tool for those examining the performance of Departments in detail.

2.35. The NAO scrutinises Statements on Internal Control, using a process of "negative assurance". This means that they examine statements made to ensure they are not inconsistent with the information gathered during the course of their audit work. The new processes put in place in Departments will ensure that in their review of the work of the Board, the NAO will have access to material covering information risk.

2.36. The Information Commissioner has the power to carry out spot checks on Departments, with the first checks currently being planned. In future, such checks will be informed by the audit trail outlined above.

2.37. Government will incorporate greater scrutiny into its Whitehall processes by:

- building information risk handling into the Capability Review process, carried out on all Government Departments. Capability Reviews are conducted by a team of external reviewers drawn from the private sector, the wider public sector and Government Departments to examine how well equipped Departments are to meet their delivery challenges;
- increasing specific Department to Department scrutiny by widening existing practice under which Departments may request of others additional assurance about the protections that others have in place. This is currently carried out under the auspices of the Office of the Government Chief Information Officer and specifically related to ICT, but will be widened to cover broader information assurance issues; and
- increasing the focus and resource in CESG devoted to critical examination of Departmental systems, through the peer review processes mentioned above.

2.38. The work of the Information Commissioner and the NAO will mean that Parliament and others will be better able to monitor progress. To reinforce this, Government is introducing additional requirements on Departments to report directly on their actions and performance.

2.39. The public are entitled to understand how the information held about them is being handled and Parliament needs to be able to hold Government to account. At the same time, arrangements should not be so transparent as to help those seeking to exploit system vulnerabilities.

2.40. Similarly, there is a clear need for more robust performance monitoring, to reflect the seriousness of the issues. But a monitoring regime that was too draconian would bring its own problems. One risk is that staff and managers could become risk-averse in handling any data, meaning that innovation and even the conduct of ordinary business would be affected. A second risk could be that individuals may become unwilling to admit to errors. This would critically undermine the ability of organisations to recover from incidents, learn lessons, or to alert individuals whose information may be compromised.

2.41. In order to strike the appropriate balance the Government has committed to report on information breaches in summary form in Departments' annual reporting. The first such material will be included in annual reporting for 2007/08. There are two exceptions to this: when the interests of those affected are best served through public announcement, or when issues are so serious that Ministers judge that their immediate accountability to Parliament overrides other considerations.

2.42. For each financial year, Departments will report:

- a summary of protected personal data related incidents formally reported to the Information Commissioner;
- a summary of centrally recorded protected personal data related incidents not formally reported to the Information Commissioner; and
- a summary statement of actions to manage information risk.

2.43. In addition to the action already announced, Government will increase the information available externally in two ways:

- all Departments will issue an Information Charter, setting out the standards that people can expect from the public body when it requests or holds their personal information, how they can get access to their personal data and what they can do if they do not think that standards are being met. Model text is set out in Annex IV; and
- in addition, all Departments will consider the scope to publish material on specific information assets that it holds, such as what information is contained and how it is used. Departments will approach this with a presumption of openness, while recognising that there will always be some information and some uses of it (for example in the national security and law enforcement arenas) where transparency must rightly be limited.

Section 3: Implementation

The conclusions from this report have been shared and acted upon by Departments as they have been developed. Implementation has started. All Departments have established new technical protections for information they hold directly. They have identified the protected personal data they hold, are rolling out encryption to protect it in transit, and have minimised the use of removable media. Departments are now working with their delivery partners to ensure that they apply the same protections.

The Government's guiding principle is that the protections outlined in this report, or their equivalent, should be in place and effective, no matter how information is held and processed for central government purposes.

Departments will work with all those involved in the delivery chain, whether they are public sector, private sector, or third sector. Progress will take time. Many public sector bodies are independent of central Government, and the material developed for central Government will need to be tailored so that it fits the audience and their requirements.

No organisation can guarantee it will never lose data, and the Government is no exception. Some of the actions set out in this document – for instance around cultural change – will take time. The specific requirements and approach to rolling them out will continue to change as services, technology and threats change. It will always be possible to improve. This means that the development of processes for improved information security will never, in that sense, be "finished". This report is a new start in a continuous and evolving process.

Departments have agreed a timetable for the initial steps for implementation over the coming year. These will be the subject of the first annual report to Parliament next year.

Central Government

3.1. As described in Annex I, Departments have worked to review and improve where necessary their own approaches to information risk and data handling. They have increased staff awareness of information risk, reminding them of their individual responsibilities as part of their organisation.

3.2. The action described in this report is being implemented as fast as possible. For Departments that deal with significant volumes of personal citizen data, this will involve working with complex and diverse delivery chains. These can include the Department, Non-Departmental Public Bodies (NDPB) and partners in the wider public or third sector, as well as contractors providing services for the Department.

3.3. The implementation approach will be phased to recognise this reality. Departments are moving fastest in respect of their own activity and the activity of those bodies where they are in a position to mandate certain ways of working. Where Departments can require the use of new measures, or higher standards where those are judged necessary, they will do so.

3.4. Where Departments cannot require the use of new measures throughout their area of responsibility immediately, they will seek to influence their delivery chain partners.

3.5. Many Government Departments engage with private sector companies to contract out elements of the services they provide, or to provide the Departments themselves with services which support their organisations. Contractors will, as part of their service provision, handle information belonging to the Department or to the public for whom the Department serves. Departments will build into new contracts the new requirements set out in this report. In addition, Departments are working with contractors under existing contracts to apply the same controls and to monitor their performance. Contact so far with contractors suggests that they recognise the shared interest in achieving high levels of data security.

3.6. The Office of Government Commerce (OGC) is updating the security clauses within its model ICT contract for services, which Departments will use to provide assurance that any contractor will have processes in place which comply with the new cross-Government requirements. In addition, Departments will set out their requirements where those go further.

3.7. Many of the specific controls to enhance protection for personal data are already in place in Departments themselves. All Departments have:

- formalised the role of SIRO;
- identified what personal data are held and used within the Department itself that falls into the new definition of "protected personal data";
- established procedures and policies to ensure such data are handled as if they are protectively marked;
- an encryption programme for such data, where it is on removable media, except where that is not possible, for example because of the need to access back-ups;
- where such data are stored electronically, minimised the use of removable media and the amount of data transferred to them, and minimised the user rights to copy files onto such media;
- introduced new arrangements where needed for secure disposal from the Department of paper and electronic records; and
- reviewed procedures for reporting information risk incidents.

3.8. Departments are undertaking a further set of activities, including:

- appointing Information Asset Owners;
- formalising their information risk policy, to reflect the actions in this report;
- rolling out protection for personal data beyond the Departments themselves to their delivery partners for which Departments can mandate use of specific measures;
- amending HR policies and guidance as necessary;
- introducing cultural change plans;
- publishing Information Charters; and
- compiling material on breaches for Departmental accounts, for 07/08 and previous years where possible.

3.9. From July:

- Information Asset Owners will review the position on their information assets, and perform their roles fully;
- new systems containing protected personal data will be subject to mandated accreditation, and build in greater access control and logging;
- standard contract clauses on information assurance will be incorporated into contracts; and
- Privacy Impact Assessments will be used and monitored.

3.10. Departments will have started their mandatory training by the end of October 2008. This timing is to allow them to develop and tailor materials as needed.

3.11. Other steps, including the deployment of penetration testing will take place during 2008/09. The first full annual assessments of progress will take place following the end of 2008/09 and be reflected in the first annual Cabinet Office Report on overall progress.

3.12. As set out in the Interim Report, Government is putting in place a programme to tighten procedures for data held overseas. This will combine controls reflecting the actions set out in this report, and through case-by-case examination by experts from the CESG, and Office of Government Commerce, with support as necessary from the Ministry of Justice.

3.13. Ministerial overview of progress will be provided through:

- Ministerial action in individual Departments;
- the Minister with responsibility for Information Rights at the Ministry of Justice;
- the Minister for the Cabinet Office and Chancellor of the Duchy of Lancaster responsible for Cabinet Office functions; and
- Paul Murphy, Secretary of State for Wales, chairing the Cabinet Sub-Committee on Personal Data Security.

The wider public sector

3.14. The work underway by some central Government Departments will influence some practices in the wider public sector.

3.15. In parallel, recognising that data security challenges are real for other public sector bodies, Government wishes to encourage others to consider adopting similar approaches themselves. As a result, the material here has been shared as it has been developed with other interested parties.

3.16. The Devolved Administrations have taken forward action and will make their own announcements. The Government will continue to work with the Devolved Administrations as the work is taken forward.

3.17. Departments are working on specific issues with partners in the wider public sector, to apply the new measures.

3.18. The Local Government Association is producing equivalent material and approaches for local government as a whole. This work is expected to be completed by the end of summer 2008. The Information Commissioner has indicated his willingness to support the result of that work as good practice, meaning that implementation would be subject to monitoring by the Audit Commission.

3.19. The Government supports this work, while recognising the need for local government to find solutions that reflect their situation, and is grateful for the Information Commissioner's support.

Reporting progress

3.20. Because of the rapid changes both in technology and in the threat to Government-held data, this work has sought to consider not only how to respond to recent losses, but also to establish a strong position from which to tackle future challenges.

3.21. Some of the actions have been about establishing standards, roles and responsibilities, but above all, this requires a culture shift. Changing the way leadership and staff think about the value and handling of information in all forms will take time to set in place, although significant progress has already been made in establishing these changes.

3.22. Departments will be reporting on progress to date in their own annual reports. Cabinet Office will follow these with the first annual reporting on the issue as a whole from Government following the end of 2008/09.

Annex I: Action taken in individual Departments

The HMRC data loss started an intensive process as all Departments re-examined their data practices under the auspices of this work. The Interim Report, published in December, summarised action taken across Government. This work has continued and broadened. This Annex provides an updated summary.

All Departments have initiated a program of cultural change in their organisations, looking at the current awareness of staff regarding data handling and information risk, and reminded staff of their responsibilities to handle information carefully. All Departments have undertaken the initial stages of implementation of the new technical and process measures to protect personal information.

I.1. The Cabinet Office (CO) has reviewed its internal security policies and procedures including those which specifically deal with the secure handling of information and protected personal data. The CO has ensured that these policies are compliant with the requirements of this report, specifically regarding limiting the use of removable media to the minimum necessary for business operation and providing encryption on any necessary non-encrypted media devices. A programme of encryption of all non-encrypted stand alone PCs used within the CO will be completed by the end of July 2008. Heads of business units in the Department have been asked to ensure and confirm that all their staff are aware of the existing policies and procedures which have been included in the Department's own security manual. CO departmental data copying continues to be audited by an automated software product. The CO continues to monitor that its procedures and systems remain compliant with the Manual of Protective Security and any other centrally provided advice. An additional exercise is being undertaken immediately (the Omand Review) to ensure that the CO's procedures, particularly concerning hard copy classified material, and the disposal of classified waste, are as effective as possible.

I.2. The Crown Prosecution Service (CPS) has reviewed and significantly changed write access to portable media. It is now only permissible to download data from the CPS system to portable media with the explicit permission of the IT Security Officer. An encryption programme for the hard drives of laptops containing personal data was completed by the end of May 2008. A review of back up tape procedures has taken place and written assurances that they are secure in transit and when stored has been provided by local managers. A Data and Information Integrity Audit has been completed with no significant issues being identified. Further work is on-going to assess and reduce risk and strengthen information risk governance, covering both personal data and other sensitive information. This will be completed during the next financial year utilising the ISO 27001 compliance programme.

I.3. The Department for Business Enterprise and Regulatory Reform (BERR) has undertaken an internal review to ensure best practice is understood across the BERR family and with delivery partners to ensure consistency and best practice in data handling security and management. Data governance arrangements have been strengthened with the appointment of senior civil service data owners. A network of Group Data Champions has also been established for liaison between the business, the data owners and BERR's delivery partners (including NDPBs).

I.4. The Department for Children, Schools and Families (DCSF) has completed a wide ranging review of security covering technology, culture, governance, data sharing procedures (including those of its

delivery partners) and physical security. Deloitte has completed an independent review of the DCSF ContactPoint system. Both review reports show no obvious flaws in current systems and procedures, but have identified a number of opportunities for improvement. The new actions in this report are being implemented quickly in the Department. Strong controls remain in place covering the use of laptops and removable media. DCSF staff and partner organisations' security responsibilities continue to be reinforced by the Permanent Secretary and through management action, stronger guidance, and training. DCSF's governance framework is monitoring and ensuring progress and pace.

I.5. The Department for Communities and Local Government (CLG) has reviewed its processes and put in place a range of additional measures to further improve its data handling processes. Of particular note CLG has recently rolled out an updated Knowledge Management Strategy, including guidance on responsible data handling, to staff. Contractors and partners have been reminded of their responsibility in this area and the CIO has written to all his senior civil service colleagues. A new laptop solution has also been recently rolled out which is fully encrypted. Access policies to key systems with personal data on them have been reviewed and a code of conduct issued to all staff that have access to systems containing personal data. The wider Communities Group are carrying out similar activities with their staff and delivery partners. CLG will continue to lead and monitor this activity across the group to ensure that minimum requirements are always met or exceeded. Where potential risks have been identified either in the Group or with delivery partners remedial measures are being put in place. Communities and Local Government is working with the Local Government Association and the Cabinet Office to ensure local authorities have access to expert information assurance advice and best practice guidance is issued.

I.6. The Department for Culture, Media and Sport's (DCMS) information management strategy is still under review. The area will shortly be considered by both the Audit Committee and the Department's Board. Draft principles for ensuring that information assurance and business risk form part of the Department's leadership culture have been published. Staff have been reminded of guidance and policies and an independent IT security audit has examined compliance. Encryption of laptops is underway, and completed for those that may be used for holding personal data. NDPBs have been informed of the new policy on the protection of data – DCMS will run a related seminar for NDPBs and delivery partners.

I.7. The Department for Environment, Food and Rural Affairs (DEFRA) has raised awareness of existing policies, procedures and good practice relevant to the use and storage of protected personal and other sensitive information. Staff across the DEFRA network have been reminded about their personal obligation to observe the existing guidance on handling information. This is being embedded through new information management accountabilities now being put in place, including a Board-level Senior Information Risk Owner and a network of Information Asset Owners. A Project on data handling procedures has been set up to deliver enhanced information assurance in DEFRA and its delivery network. A Project Board (consisting of representative key delivery bodies, business areas holding significant personal data and information risk experts) has been established to support the work to implement the requirements in the Data Handling Review. This includes ensuring appropriate accountabilities and responsibilities for information assurance; putting in place technical and other measures to ensure that protected personal and other sensitive information is adequately secured (including the roll out of a new fully encrypted laptop solution which will be completed by the end of 2008); and will also continue to review and improve, where necessary, existing security policies and procedures to ensure staff understand how data should be classified, stored, and handled.

I.8. The Department of Health (DH) has started implementation of the new actions in this report. Progress across the Department and its delivery bodies is being secured and monitored by a dedicated Programme Board. Reports on progress have been

made to the Departmental Board and to the Audit Committee. Where the protections developed for use inside Government are not practicable for patient facing services within the NHS, work is in progress to ensure that equivalent safeguards are put in place. Full compliance will take some time, and must be achieved in a way that does not place patients at risk. For example the transmission of personal data to receiving A&E units by ambulance crews needs to be made more secure but prevention of transmission in the interim would have been detrimental to patient care. Individual NHS Trusts have been asked to make a local judgement on the balance of risk to patient care against risk to personal data security in determining whether existing data sharing for particular purposes should continue whilst the steps required to secure data transfers are taken.

I.9. The Department for Innovation, Universities and Skills (DIUS) adopted procedures from its two predecessor departments whilst developing its own approach. DIUS's IT policy is standardised on laptops with full disc encryption, which places the Department in a strong position regarding information security. But DIUS commissioned an independent review in support of its data handling procedures. An implementation plan has been formulated allowing the development of Department-wide policies and procedures to meet the outcomes for this report, and good progress is being made. The DIUS Audit and Risk Committee has met to discuss information assurance issues, and will continue to take an active interest in this area. Furthermore, DIUS has held the first in a series of information assurance forums to enable its delivery partners to hear and share best practice from each other and from other experts. This is part of an ongoing dialogue with delivery partners to ensure an appropriate level of information assurance throughout the DIUS delivery chain.

I.10. The Department for International Development (DfID) achieved accreditation to ISO 27001 in March 2008. The Department does not hold large amounts of personal data relating to members of the public, it does hold significant volumes of commercial and security data. It takes a risk-based approach to information security and is reviewing its decisions on the controls over the storage, retrieval and transmission of all sensitive data.

I.11. The Department for Transport (DfT) announced in December a series of measures to improve the security of the personal information it holds. Since then, further progress has been made, including encryption of laptops, further replacement of discs with electronic transfer, new procedures on bulk transfer of forms and letters containing personal data, and work with IT suppliers to ensure systems and processes are robust and secure. Existing procedures have continued to be reviewed and improved, reflecting both internal lessons and the conclusions of this report.

I.12. The Department for Work and Pensions (DWP) has introduced improved controls over the physical transfer of data on removable media. These include the introduction of new more stringent procedures for Departmental staff and Service Providers, including refreshed guidance and a secure same-day courier service. All laptops in the Department have been replaced with fully encrypted laptops and non-encrypted devices are electronically barred from connecting to the network. DWP has introduced a fast-track project for the encryption of data transfers that cannot be done electronically. The Department has set up a dedicated project, led by a senior executive, to implement a number of other actions to improve data handling.

I.13. The Foreign and Commonwealth Office (FCO) issued reinforced instructions on data security and data protection issues to UKvisas staff in December 2007. New instructions on data handling and data security, in particular laptops and drives containing personal data, were issued in January and have been updated since. A centralised system for reporting incidents involving personal data has now been put in place. Additional guidance on the Data Protection Act, to emphasise and advise on its practical implications, has been circulated to the key units. As part of the FCO role in providing a global network for Government, FCO are undertaking a review of its worldwide mail services and will be acting on its recommendations.

I.14. The Home Office (HO), before

the HMRC data loss, had already begun a review of its data security. This is being extended to take account of the issues arising from this report work. In parallel the HO has taken five further steps to tighten arrangements. New guidance has been issued to staff on the protective marking of documents and on their responsibilities under the Data Protection Act. Key data exchanges have been re-examined, with a view to increasing security. Data handling has been included in the compliance audit programme, to check that managers are following guidance. A new senior post has been created to support the SIRO and CIO on information management issues, including data handling procedures. Finally, the HO has established a new information assurance programme to ensure the implementation of the new mandatory minimum standards for the protection of personal data.

I.15. HM Revenue and Customs (HMRC) has continued to strengthen its data security arrangements since the Child Benefit data loss incident. It is co-operating fully with the external reviews, including the review by Kieran Poynter, and other investigations looking at the specifics of the incident, as well as wider data security issues. HMRC has taken significant steps to strengthen its data security arrangements in the short term and has now established and introduced a wide-ranging Departmental Data Security Programme to identify and drive forward delivery of further improvements in a structured way. This programme will incorporate any further work that may be required following receipt of the final Poynter Review report which is expected to be received in the first half of 2008 increased emphasis on compliance.

I.16. HM Treasury (HMT) is enhancing its staff education and training in security backed by senior management leadership and increased emphasis on compliance. In the light of the recent incident in which documents were lost, HMT has undertaken an immediate investigation and updated policies and procedures in light of the lessons learnt. The documents have been assessed to ensure that there was no breach of the Data Protection Act and there was no personal data associated with this incident.

I.17. The Ministry of Defence (MoD), following a loss of a laptop on 9 January 2008, commissioned an independent review by Sir Edmund Burton into the incident and lessons to be learned. Notwithstanding this review, the Chief of the Defence Staff and the Permanent Secretary have initiated a campaign across the Department to raise awareness as well as appointing a Departmental Head of Information Assurance and Data Protection. Further action has included: assigning responsibility for ensuring rigorous information assurance standards for systems outside the central accreditation and assurance system to the Departmental Security Officer; briefing information risk management to Integrated Project Team leaders; engaging with industry partners over the implications of this report; and putting in train the full-disc encryption of some 20,000 laptops across the Department. The Department is producing a consolidated programme to implement the recommendations of the Burton and Data Handling reviews.

I.18. The Ministry of Justice (MoJ) is continuing to make progress on all the actions identified in its December report. This includes ongoing communications to all staff about information management and security, launching a new Data Protection and Freedom of Information network, accompanied by new guidance about those Acts provisions and requirements, and work to review central induction and training programmes. Training delivery will reflect local solutions and included the roll-out from May 2008 of an on-line training package on security awareness and procedures in the National Offender Management Service (NOMS). A Ministry-wide information assurance programme is now in place to take forward implementation of the recommendations of this report.

I.19. The Northern Ireland Office (NIO) have completed a detailed review of their Data Handling and Information Assurance Policies and are satisfied that they comply with HMG policies/standards and ISO 27001. Policies will be continuously monitored to ensure compliance with any changes proposed or "lessons learnt" centrally. The Department has introduced new governance arrangements; an Accreditation Panel of key users and a

Senior Risk Owners Council under the chairmanship of the SIRO have been established. The Department is complying with central guidance vis-à-vis removable media unencrypted laptops holding personal or protectively marked material. All staff in the NIO and satellite bodies are receiving refresher training for Data Handling and Information Assurance.

Annex II: Timeline

II.1. By end April 2008, all Departments had completed initial measures for the protection of personal data.

II.2. Departments will include summary material on information risk in their annual reporting, through the Management Commentary to their resource accounts for 2007/08, as those are issued.

II.3. Departments are currently:

- completing roll-out of new protection through their delivery chains, where they can require the use of particular measures;
- putting plans in place to encourage use of protective measures where they cannot require their use;
- completing initial changes to Departmental HR policies;
- putting in place cultural change plans;
- allocating responsibility to Information Asset Owners;
- formalising their information risk policy in light of the material in this report; and
- publishing their Information Charter.

II.4. From July 2008 onwards:

- new systems containing protected personal data will be accredited;
- new contracts will include standard contract clauses including new protection;
- Privacy Impact Assessments will be completed;
- greater access control will be introduced; and
- penetration testing will be in place.

II.5. By October 2008:

- Information Asset Owners will have their controls operating for their information assets; and
- mandatory training for data users and senior managers will have commenced, with its first cycle to have been completed within 12 months, so that the current population will have been covered in that time.

II.6. During the 2008/09 reporting year, Departments will conduct their annual assessments, to inform their Accounting Officer's judgement in the Statement on Internal Control.

II.7. Following the end of the 2008/09 reporting year, Cabinet Office will provide to Parliament material on information risk as a whole.

Annex III: Conduct of the work

This work for this report was started in November 2007. An Interim Progress Report was published on 17 December 2007.

Governance

Members of the steering group for the work were: Gus O'Donnell (Chair); Natalie Ceeney, The National Archives; Alexis Cleveland, CO; James Crosby; Karen Dunnell, ONS; John Fiennes, CO; Robert Hannigan, CO; Helen Kilpatrick, HO; Leigh Lewis, DWP; David Pepper GCHQ; Ian Watmore, DIUS; Chris Wright, CO; and Tim Wright, DCSF.

In addition, a 'Red Team' was established to examine material. The team was: Charles Branch, BERR; Mara Broome, MoJ; Chris Bywater, DWP; David Chilver, HMRC; John Cook, MoD; Belinda Crowe, MoJ; Stephen Hickey, DfT; Colin Hurd, DCSF; Richard Jeavons, DH; Robin Pape, HO; Clive Porro, DEFRA; and Linda Wishart, DH.

Advice and expertise

The team are grateful for the help and support received from:

- Richard Thomas, the Information Commissioner, and his Office;
- The Local Government Association; and
- the Financial Services Authority.

The team benefited from input from:

- Professor John Beddington, Chief Scientific Advisor;
- Andy Clark, Head of Detica Forensics;
- Professor Brian Collins, DfT;
- Professor William Dutton, Oxford Internet Institute;
- Robert Ghanea-Hercock, BT;
- Professor Wendy Hall, School of Electronics and Computer Science, University of Southampton;
- Professor Keith Jeffery, Science and Technology Research Council;
- Professor Cliff Jones, Newcastle University;
- Professor John Pethica, Department of Materials, Oxford University;
- Professor Angela Sasse, University College London.

For their help in assessing private sector good practice, the team would like to thank:

- BT Group;
- Deloitte;
- Equifax plc;
- Experian Ltd;
- HBOS plc;
- Home Retail Group;
- Microsoft Corporation;
- Pfizer Ltd;
- Sapior Ltd; and
- Serco Consulting.

Annex IV: Information charter

This annex contains a standard information charter, which will be tailored by individual Departments and published.

We need to handle personal information about you so that we can provide better services for you. This is how we look after that information.

When we ask you for personal information, we promise:

- to make sure you know why we need it;
- to ask only for what we need, and not to collect too much or irrelevant information;
- to protect it and make sure nobody has access to it who shouldn't;
- to let you know if we share it with other organisations to give you better public services - and if you can say no;
- to make sure we don't keep it longer than necessary; and
- not to make your personal information available for commercial use without your permission.

In return, we ask you to:

- give us accurate information; and
- tell us as soon as possible if there are any changes, such as a new address.

This helps us to keep your information reliable and up to date.

You can get more details on:

- how to find out what information we hold about you and how to ask us to correct any mistakes;
- agreements we have with other organisations for sharing information;
- circumstances where we can pass on your personal information without telling you, for example, to prevent and detect crime or to produce anonymised statistics;
- our instructions to staff on how to collect, use and delete your personal information;
- how we check the information we hold is accurate and up to date; and
- how to make a complaint.

FOR MORE INFORMATION, PLEASE CONTACT: XXXXXX

When we ask you for information, we will keep to the law, including the Data Protection Act 1998. For independent advice about data protection, privacy and data-sharing issues, you can contact the Information Commissioner at: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Phone: 08456 30 60 60 or 01625 54 57 45 Fax: 01625 524510
Website: www.ico.gov.uk

Annex V: Cross-references to other work

This annex provides a summary of recommendations from each of the following reports and how each of these recommendations has been or will be addressed.

Joint Committee on Human Rights, Data Protection and Human Rights Report (Fourteenth Report of Session 2007-08)

1. 'Government must show that any proposal for data sharing is both justifiable and proportionate, and that appropriate safeguards are in place to ensure that personal data is not disclosed arbitrarily but only in circumstances where it is proportionate to do so.' (paragraph 14 of JCHR)

*Agree. The provisions in this report should assist in this area. The use of Privacy Impact Assessments (**www.ico.co.uk**) should ensure that privacy issues are factored in at early stages of development. Issues around data sharing are also being considered in the Walport / Thomas review.*

2. 'Where there is a demonstrable need to legislate to permit data sharing between public sector bodies, or between public and private sector bodies, the Government's intentions should be set out clearly in primary legislation.' (paragraph 20)

Issues around data sharing are being considered in the Walport / Thomas review. (In some instances, Government does set out specific provisions in primary legislation.) Data protection safeguards are enshrined in the Data Protection Act. Whether data sharing provisions are best set out in primary or secondary legislation will depend on the context of the legislation and the data sharing involved. The efficient use of codes of practice may provide a more pragmatic and effective approach in the form of practical and detailed guidance to front line staff who manage and handle information than can be offered solely in the form of provisions set out in primary legislation.

3. 'There should be inter-departmental coordination to share best practice and help deal with the fall-out from significant breaches of data protection by Departments.' (paragraph 26)

Agree. Cabinet Office has always sought to ensure that Departments are able to learn from each other, including when things go wrong. It will continue to do so. Departments will also be supported through peer review mechanisms.

4. 'The role of the data protection minister should be enhanced from just overseeing the data protection legislation to championing best practice and ensuring that lessons are learned from breaches.' (paragraph 26)

The data protection minister and the Ministry of Justice already play this wider role. The data protection minister and others will participate in the collective work of the Committee on Personal Data Security, (DA(PDS)) to ensure that Government follows through its commitments in this report.

5. 'The Government should acknowledge the close connection between data protection and human rights; and explain how it proposes to ensure that a culture of respect for personal data is fostered throughout Government.'(paragraph 35)

This report sets out actions to ensure that a culture of respect for personal data is fostered and valued, This will be achieved by

greater transparency as Departments will report annually on information assurance issues but also throughout the whole of Government, through assessing privacy impacts at an early stage, through culture change and training, and through ensuring that HR systems support good performance.

6. 'Support proposals to enhance the Commissioner's powers and resources at his disposal to ensure that he can discharge his responsibilities more effectively.' (paragraph 39)

The Government made clear in publishing the interim report for this work that it was committed to providing the Information Commissioner with the power to conduct spot checks and the Data Protection Act has been recently amended to confer, on the Information Commissioner, a power to impose a monetary penalty on a data controller where the Information Commissioner is satisfied that a serious contravention of the data protection principles has occurred. Spot checks by the Information Commissioner of government departments are due to commence over the coming months.

7. 'Government should take action to foster a positive culture for the protection of personal data by public sector bodies.' (paragraph 50)

See the answer to recommendation 5 above. In addition, Government is improving accountability mechanisms, and strengthening scrutiny of performance.

Select Committee on Justice First Report, 3 January 2008

1. 'The introduction of new laws making significant security breaches, where reckless or repeated, a criminal offence.'

Government introduced a new monetary penalty in the Criminal Justice and Immigration Act (2008) which will give the Information Commissioner the discretion to serve notice on a data controller who has seriously contravened the data protection principles. Government will take a considered view on what further measures are necessary to strengthen the protection of personal data in light of the recommendations of the various data protection reviews.

2. 'New reporting requirements that would require companies to report losses of data.'

This issue relates to the wider legal framework, and Government will consider it in the light of the conclusions of the Walport / Thomas review due shortly.

3. 'Quick implementation of the new enforcement powers for the Information Commissioner to conduct unannounced spot checks on Government Departments' data systems.'

No legislation is required to permit the Information Commissioner to conduct spot checks on Government Departments. Government has given its consent for such spot checks to be conducted. The Information Commissioner will lead on how and when such spot checks take place.

4. 'Proper resources for the Office of the Information Commissioner.'

Government will take a considered view on what further measures if any are necessary to strengthen the protection of personal data in light of the recommendations of the various data protection reviews. This will include consideration of the funding arrangements for the Information Commissioner's Office.

Protecting Government Information: Independent review of Government information assurance, by Nick Coleman

Government accepts the thrust of each of the key recommendations in the report. Individual responses are set out below.

1. Government should create a vision for information assurance and that this vision should be incorporated into existing vision statements; laying out for citizens and other stakeholders what it considers are acceptable parameters for the sharing, managing and protecting of information held and managed by Government.

   A vision for information assurance was set out in the National Information Assurance Strategy, published in June 2007. In the course of this work, Government has specified a minimum definition of personal information that should be protected, and the minimum level of protection required for it. The establishment of Information Charters should also support transparency. Government will consider the need for further action in the light of the Walport / Thomas review due shortly.

2. Create a new approach for reviewing and managing information risks across Government. Enable new mechanisms to enhance the effectiveness of information risk management including a central facility for sharing risk information.

   This will be taken forward by Cabinet Office, working with Departments, as part of the work to embed information risk management practice across Government. Cabinet Office will receive annual assessments from Departments, and use those to develop a cross-Government view of the risks being faced by Departments, to inform work on common standards or other action. Departments will capture risk information for critical assets.

3. Mandate board owners to report quarterly on information risks and performance backed up by an annual audit of Department's capabilities. Within this, establish clear metrics for managing performance of suppliers.

   Quarterly reporting on information risk and annual assessment are part of the new approach in place for all Departments. As part of the development of their information risk policy, Departments will consider how best to ensure high levels of data security when working with suppliers. Cabinet Office will consider the case for further specific metrics, including for managing performance of suppliers, as part of work on future development of cross-Government requirements.

4. Provide the Prime Minister with a summary of information assurance across Government and associated spending required to deliver cross Government security associated with information assurance.

   The Prime Minister will be provided with a summary of information assurance across Government as part of the preparations for the annual report to Parliament on information risk. This will set out the level of "common good" spending.

5. Simplify the complexity of the twenty five plus working groups and structures in this area. Enable one central mechanism for developing coordinated joint working for sharing best practice and establishing information assurance priorities across Departments and agencies.

   While there will always be a significant range of groups with an interest in this area, this report recognises the need to simplify and streamline arrangements, and for Departments to learn from each other and co-operate where

that makes sense.

6. Create clear mandatory policy rules on security across Government. Define minimum standards that Departments sign up to. Enable independent monitoring for compliance.

   The definition of clear mandatory policy and simple minimum standards has been taken forward by this report. Independent monitoring will be provided by the National Audit Office and Information Commissioner, in addition to peer review. The requirements for Departments will need to evolve in the future.

7. Tackle identity management challenges through mandating the use of Privacy Impact Assessments. Specify standards of protection for identity registration, management and use in Government and the wider public sector.

   Government is adopting Privacy Impact Assessments. Standards of protection for identity management will be the subject of on-going work. The use of Information Charters should improve transparency to the citizen.

8. Mandate professional certification for those working in information assurance in every Government Department across key defined roles. Ensure citizens, employees and other stakeholders are educated on information assurance and what is expected of them.

   Agree with the need for professional certification for individuals working in roles with technical information assurance content. Cabinet Office will take forward work to increase professional capacity, and ensure that the right links are made with the closely related areas of IT and knowledge and information management. Government has not mandated professional requirements for named roles, or additional remuneration, because of the widely different way in which Departments approach their business.

9. Measure security through audit and monitoring to a defined standard. Mandate the reporting of incidents to an independent organisation responsible for capturing incidents and ensuring investigations are conducted to a given standard and lessons are learned.

   Agree with the need to measure security through audit. This will be done against cross-Government standards. Reporting of incidents will take place to the Information Commissioner, who will take enforcement action where justified and appropriate. CESG, the National Technical Authority, will be one of a number of bodies able to trigger the peer review mechanism between Departments. The responsibility for ensuring investigations are carried out appropriately and lessons are learned should continue with the individual Department, subject to the scrutiny mechanisms set out in this report.

10. Have an independent oversight capability retained by Government who can be called upon to give independent oversight and advice on information assurance to give stakeholders confidence. Provide this capability in addition to the formal regulatory roles that exist outside Government.

    The formal regulatory role exercised by the Information Commissioner will remain important. Oversight will be provided by the NAO, in the course of their work. Additional independent input will be provided by CESG, through peer review, and other independent experts. Cabinet Office will continue to seek advice on best practice from independent experts.

Fifth Report from the House of Lords Science and Technology Committee, Session 2006-07, HL Paper 165, 24 July 2007

1. ‘Government should ensure that the right incentives are in place to persuade businesses to take the necessary steps to act proportionately to protect personal data.’

This relates to wider data sharing issues outside the scope of this review, and Government will consider it in the light of the conclusions of the Walport / Thomas review due shortly.

2. Government should introduce legislation, consistent with the principles enshrined in common law and, with regard to checks, in the Bills of Exchange Act (1882), to establish the principle that banks should be held liable for losses incurred as a result of electronic fraud.

This issue relates to the wider legal framework, and Government will consider it in the light of the conclusions of the Walport / Thomas review due shortly.

3. Government should begin consultation on the scope of a data security breach notification law as a matter of urgency. The law should incorporate the following key elements:
    - workable definitions of data security breaches, covering both a threshold for the sensitivity of the data lost, and criteria for the accessibility of that data;
    - a mandatory and uniform central reporting system; clear rules on form and content of notification letters, which must state clearly the nature of the breach and provide advice on the steps that individuals should take to deal with it;

This issue relates to the wider legal framework, and Government will consider it in the light of the conclusions of the Walport / Thomas review due shortly.

4. Government should examine as a matter of urgency the effectiveness of the Information Commissioner's Office in enforcing good standards of data protection across the business community. The Commissioner is currently handicapped in his work by lack of resources; a cumbersome "two strike" enforcement process; and inadequate penalties upon conviction.

The Government introduced a new monetary penalty in the Criminal Justice and Immigration Act which will give the Information Commissioner the discretion to serve notice on a data controller who has seriously contravened the data protection principles. Government will take a considered view on what if any further measures are necessary to strengthen the protection of personal data in light of the recommendations of the various data protection reviews.

5. Government should reconsider the tariffs for the whole of the data protection regime, while also addressing resources and enforcement procedures as well. These should include the power to conduct random audits of the security measures in place in businesses and other organisations holding personal data.

See above.

6. Government should introduce amendments to the criminal law, explicitly to criminalise the sale or purchase of the services of a ‘botnet’, regardless of the use to which it is put.

The Computer Misuse Act (1990) has been amended through the Police & Justice Act (2006) to provide a legal base to tackle this problem. The Crown Prosecution Office has produced advice for courts to ensure that the legitimate use of such articles is not penalised. Work to implement the Police and Criminal Justice Act began in April 2008.

7. Government should, in partnership with the Association of Chief Police Officers and the Serious Organised Crime Agency, develop a unified, web-based reporting system for e-crime (including recommendations on reporting to banks of online fraud; establishment of computer forensic laboratories, HO to introduce Police Central e-crime Unit; ratify the Council of Europe CyberCrime Convention; issue guidance to courts on internet crime)

The Government takes the threat of e-crime seriously. The Government has provided £15m over the next three years to set up the National Fraud Reporting Centre, which will help identify and analyse electronic fraud. The Government will shortly be discussing with law enforcement agencies how best to tackle the issue of electronic fraud. The Government fully intends to ratify the CoE Cybercrime Convention, and work on this began in April 2008.