DATA HANDLING IN GOVERNMENT

JUNE 2008

The Scottish Government

DATA HANDLING IN GOVERNMENT

EXECUTIVE SUMMARY

1. On 23 November 2007, the Scottish Government announced that it would conduct a coordinated review of information security policies and data handling arrangements in Scotland. The Scottish Government's Strategic Board asked the Director-General Justice and Communities to co-ordinate this review, supported by a review team drawing together key interests across the Scottish Government.

2. The review was conducted in 2 phases. Phase 1 focused on the current information security policies and data handling arrangements and how these were being implemented across central government, particularly for personal data. Phase 2 sought to identify good practice and make recommendations based on the findings from Phase 1 and drawing on the emerging findings across the wider public sector in Scotland, from the other Devolved Administrations and across the UK as a whole.

3. A high percentage of respondents were able to confirm that they had good or very good policies or procedures for information management, data protection and sharing. The leadership scores indicated that respondents were taking the governance aspects of information management, data handling and sharing seriously.

4. The Scottish Government itself holds substantial information on citizens and businesses, and to deliver public services effectively and efficiently, information needs to be shared between different parts of Government. However, citizens have a right to expect the information that they provide to Government will be held securely and used appropriately and it is essential to retain public trust in Government's use of information. The key recommendations from the review are:

- The Scottish Government should broaden its leadership role and act as the source of centralised, authoritative guidance and assistance for Scottish public bodies.
- The Scottish Government should be proactive in ensuring compliance with security standards, and actively monitor compliance through audits or health checks.
- The Scottish Government's expectations of public bodies on information security, risk management and data sharing must be clearly defined and easily accessible, and include minimum standards.
- The Scottish Government should ensure that policies and procedures do not create inefficiencies, impede data sharing or legitimate access to information, or create addition risks to the public.

5. This review has found that data security is being taken seriously across the Scottish Government and its agencies but that there is room for improvement. There is substantial good practice in Scotland but there have also been a few breaches of security, which are damaging to public confidence. Smaller organisations with smaller holdings of data generally found it more difficult to devote adequate resources to delivering their information security responsibilities than large organisations holding substantial quantities of data.

6. The assessment of the review team was that further measures were needed to improve the security of sensitive information. In line with the conclusion of the earlier update and the stated views of the respondents to the questionnaire, we believe that there is strong demand, and a strong case for, the Scottish Government acting as a source of centralised, authoritative guidance and assistance for Scottish public bodies – rather than individual bodies devising their own policies, procedures and guidance.

7. Most respondents had an information security policy, although a minority did not have a documented and approved information management strategy. Most respondents needed to do more to communicate well and regularly with their staff about information management, data protection and data sharing. The challenge to the Scottish Government is to foster a culture of continuous improvement in effective risk management while supporting service delivery and enabling legitimate information sharing.

Introduction

1. On 23 November 2007, the Scottish Government announced that it would conduct a coordinated review of information security policies and data handling arrangements in Scotland. The Scottish Government's Strategic Board asked the Director-General Justice and Communities to co-ordinate this review, supported by a review team drawing together key interests across the Scottish Government.

2. The review team were asked to consider:

- the procedures currently in place for the protection of data;
- their consistency with Government wide standards and policies; and
- the arrangements for ensuring that policies and procedures were being fully and correctly implemented.

The team was also asked to identify areas of good practice and to make recommendations for improvement.

Scope

3. The scope of the Review covered central government in Scotland. (A full list of the bodies covered by the Review is at Annex A.) The Review operated on the basis that organisations which were not part of central government were conducting their own reviews but that the Scottish Government review would work with the wider public sector to secure assurance on information security procedures and processes across the Scottish public sector. The Scottish Government therefore contacted Local Authority Chief Executives, the Association of Chief Police Officers in Scotland (ACPOS), the Chief Fire Officers' Association (CFOA), and Universities Scotland and the Association of Scotland's Colleges, to share the review questions and assurances sought. The emerging findings of the review have been shared with the NHS in Scotland and with the National Data Sharing Forum.

4. Similar reviews were commissioned by the Cabinet Office for UK Government Departments, and by the Northern Ireland Office and the Welsh Assembly Government. Data are often shared by the various Governments in the UK, and all of the UK administrations recognised the importance of working together on this issue and are keeping one another informed of work as it progresses. Decisions about the specific recommendations arising from the reviews, and detailed risk management arrangements which flow from these, rest with the Scottish Government.

5. In addition, separate work is in hand following the loss of personal data by HM Revenue and Customs, and work is being taken forward by the UK Information Commissioner on policy issues related to sharing of personal data in both the public and private sector. We expect the results to inform further improvements in risk management procedures for personal data.

Conduct of the Data Handling Review

6. The Scottish Government Review, led by the Director-General Justice and Communities, was conducted in 2 phases. Phase 1 focused on the current information security policies and data handling arrangements and how these were being implemented across central government; particularly for personal data. Phase 2 sought to identify good practice and make recommendations based on the findings from Phase 1 and drawing on the emerging findings across the wider public sector in Scotland, from the other Devolved Administrations and across the UK as a whole.

7. This report on the findings and recommendations from the review clearly focuses on central government in Scotland. It is for individual organisations to identify, understand and manage their own business risks and the specific measures designed to improve information management within central government may not be appropriate for front line service delivery organisations. However, the good practice identified and the published standards for information risk management on which many of the recommendations are based are equally applicable across the wider public sector.

Phase 1: Process

8. The initial phase of the review considered the procedures currently in place for the protection of data and their consistency with Government wide standards and policies.

9. A detailed questionnaire, in a form consistent with that agreed by the Cabinet Office, was issued to all central government bodies, including NHSScotland, with instructions to return the completed questionnaire to the co-ordination point by 10 December 2007. The questions and assurances sought from central government agencies were also shared, for information, with Local Authority Chief Executives, ACPOS, CFOA, and educational establishments. Some multi-agency programmes involving data sharing were also included.

10. On the basis of the returns, the Permanent Secretary, Scottish Government Directors-General and the Chief Executives of Non-Ministerial Departments, Agencies and Non Departmental Public Bodies (NDPBs) were asked to satisfy themselves as Accountable Officers that the information security procedures and processes in their areas complied with the Scottish Government's security standards for access to, storage, extraction and transmission of data of a sensitive nature, in particular where this relates to personal information. Similar assurances were sought from NHS Board Chief Executives and their responses were collated by NHS Scotland and shared with the Review team.

11. All Scottish Government staff were reminded of the need to adhere to standards for protection of data and to take appropriate care of data received, stored or transmitted to other bodies. There was particular focus on the correct procedures for transfer of data on removable media, including the importance of password protection and encryption, and the safe disposal of classified waste.

Phase 1: Interim Reports

12. The returns received in December 2007 were used to inform an interim report on Data Handling to the Cabinet Secretary for Finance and Sustainable Growth. This report was completed on 14 December 2007.

13. The responses to the review of information security policies and data handling arrangements in Scotland were generally thorough, suggesting that the respondents took the exercise seriously and considered their answers in some depth. It was clear that some organisations had already initiated work to examine their systems and procedures surrounding data handling and sharing, and others confirmed that they were addressing the weaknesses identified in their completed questionnaires. Organisations were advised not to wait to address issues and the Scottish Government's security team continue to provide advice on issues as they are addressed.

14. A high percentage (74%) of respondents confirmed that they had very good, or good, policies or procedures for information management, data protection and sharing. The Leadership scores indicated that the governance aspects of information management and data handling and sharing were taken seriously by all of the respondents with responsibility held at Board or senior management levels.

15. Although most respondents had an information security policy a minority did not have a documented and approved information management strategy. This may be the reason why other questions scored less well and may be an indication that, to be effective and secure, organisational policies and principles for information management must be determined at the highest levels and communicated throughout the organisation. Most respondents needed to do more to communicate well and regularly with their staff about information management, data protection and data sharing.

16. The majority of Accountable Officers were able to satisfy themselves that there were no significant gaps in their organisation's compliance and approach to data protection and sharing. However, the analysis of the detailed responses suggested that further strengthening was required on data sharing, on policies and procedures and on risk assessment and management.

17. The majority of respondents completed risk assessments for their organisation. However, the evidence presented suggested that a number of organisations should develop risk management approaches which are holistic, regular and conducted to repeatable standards. We were pleased to note that most organisations acknowledge that they do recognise information risks; but only a small percentage were able to offer detailed quantification of their risks and their mitigation strategy. This indicates that further work is required in a number of organisations on qualifying and quantifying vulnerability to threats and on identifying the root cause of the vulnerability.

18. As part of the questionnaire, organisations were asked if they had any recommendations on current information risk management and data handling

procedures. A significant number of respondents took the opportunity to suggest mechanisms to improve the sharing of best practice. Their recommendations included:

- A request for the Scottish Government to provide leadership and act as the source of centralised, authoritative guidance and assistance for Scottish public bodies; for example by establishing overarching policies for information security, risk management and data sharing.

- The Scottish Government should be proactive in ensuring compliance with security standards, and actively monitor compliance through audits or health checks.

- The Scottish Government's expectations of public bodies on information security, risk management and data sharing must be clearly defined and easily accessible. In particular the rules and boundaries for data sharing should be explicit to ensure that there is no disparity between public sector bodies as regards their technical solutions, data handling procedures or working practices.

19. However, organisations were also very clear that any review had to ensure that policies and procedures did not impede access to information and data sharing in ways that were detrimental to the efficient operation of the business, or increased risks to the public.

20. The assessment of the interim set of survey responses confirmed that there was a need for further measures to improve the security of sensitive information and a need for more central of oversight and guidance – rather than these bodies fending for themselves and devising their own policies, procedures and guidance.

Phase 2: Process

21. Phase 2 of the review sought to examine further the responses to the data sharing questionnaire in order to:

- underline areas of immediate concern or where serious issues were uncovered;
- highlight gaps within current processes and procedures for data handling within responses collected;
- identify where follow-up action and intervention needs to take place, and finally to;
- create recommendations for remediation and improvement in the form of an action plan.

22. The second phase of the review was also intended to identify examples of good practice across the public sector in Scotland and make recommendations on improvements in risk management based on the emerging findings across the wider public sector in Scotland, from the other Devolved Administrations and across the UK as a whole. This phase of the review sought to take a broader approach to data handling and risk management; balancing the requirement to secure data

appropriately with the need to be able to share it effectively and considering the balance between local accountability and central direction.

23. In particular, the value of sharing data effectively and securely was highlighted by the example of e-Care where it is recognised that in sharing information a better service can be offered to vulnerable citizens whilst still protecting the rights of the individual. Data sharing can also contribute significantly to reducing the burden placed on respondents (individuals, households and businesses) by ensuring that individual data items are collected once but used, for legitimate purposes, many times.

Phase 2: analysis and action plan

24. We analysed the completed responses on information security policies and data handling arrangements in Scotland in detail and drew up an action plan to target areas of concern and gaps in current processes or understanding.

25. As with the interim study the responses were generally thorough. Respondents took the exercise seriously and considered their answers in some depth with the majority providing detailed, open and candid answers, reflecting the fact that there have been isolated examples of loss of data.

26. The analysis established that some of the smaller organisations that provided responses scored poorly. Further examination showed that these smaller organisations have very little data sharing compared to larger bodies such as the Scottish Government; they therefore have less well developed policies and ways of working and limited access to information assurance advice or resources.

27. A very high percentage of respondents said that they had very good, or good, policies or procedures for information management, data protection and sharing and the governance aspects of information management. Data handling and sharing were taken seriously by all of the respondents with responsibility being held at either Board or senior management levels. Of those who responded 84% shared data in some manner with 47% of these sharing data with bodies who were not Government departments. Additional work is underway to understand gaps that have been highlighted and we have an exercise planned to verify the baseline indicated by the responses in the exercise.

28. We are carrying out a follow-up review with those organisations that demonstrated low compliance through the review to determine the immediate issues and identify further remedial action. We will also audit and validate, on the basis of a random cross-section, the accuracy of responses from organisations that scored highly.

29. The vast majority of respondents acknowledged that information risks are present in their organisation, but further work is required on putting plans in place to deal with these. Every organisation faces risks; these risks can be managed so long as they are understood and measured, and there are plans for mitigation and improvement in place and are regularly reviewed.

30. The Scottish Government's security team continues to advise on approaches to data handling and are providing revised good practice on systems and procedures surrounding data handling and sharing as these are agreed. One organisation used the questionnaire to request support for helping develop an information management policy and this exercise is now underway. Other inputs included the observation that there was a need for more sharing of good practice between organisations in Scotland. The survey analysis also demonstrated interest within responding organisations in using shared services that might allow data sharing and exchange with information held centrally and accessed over secure channels. This will be followed up with the specific organisations identified.

31. The review highlighted the importance of ensuring that organisations understand the distinction between personal data handling and information handling more generally; and in particular the need to secure common understanding of what is meant by personal and/or sensitive data. A definition of a new term 'protected personal information' has been agreed by the Cabinet Office and the Information Commissioner and is included at Annex B.

Good Practice

Good Practice: eCare

32. The Scottish Government is developing the eCare framework to provide secure data sharing between agencies and professionals working with children and vulnerable people. The system is organised on a federated model, thus avoiding the risks implicit in building a national database. Instead the framework allows sharing between professionals when there is a reason to do so - to provide services. Except for when there is an over-riding legal duty to share, data sharing only takes place with the consent of the client and the sharing of data is documented and auditable.

33. Data protection has been an important principle of the framework from the outset and the eCare framework was recently a prize winner in a European competition on good practice in data protection. Protections are in place to prevent any bulk down loading of data. The system is designed so that only one record can be accessed at a time, by a professional who needs the information and has the consents to do so.

Good Practice: NHSScotland

34. The suggestions that a more centralised approach on guidance and policies for information security, risk management and data sharing across Agencies and NDPBs would be beneficial is consistent with the experience of NHSScotland. The fact that there is a widely promulgated set of standards and processes within NHSScotland has been worthwhile; their responses to the questionnaire displayed a higher degree of understanding and consistency of approach.

35. The following summary outlines the progress made in NHSScotland over recent years in relation to Information Governance, including Information security.

36. An independent review of the way in which NHSScotland uses health information was carried out by the Confidentiality and Security Advisory Group for Scotland (CSAGS) in 2002[1]. CSAGS recommended changes in practice and this has resulted in a substantial programme of work over the five years from 2002 to 2007 led by the, then, Scottish Executive Health Department (SEHD).

37. Substantial progress has now been made in implementing CSAGS recommendations. A new Code of Practice has been introduced; improved training

[1] http://www.confidentiality.scot.nhs.uk/externalresources/csags.htm

and information for staff is available; and a national framework of Information Governance has been established. The main elements of this are:

- National Information Governance Standards[2] - these form part of NHSScotland's Clinical Governance and Risk Management Standards
- A reporting toolkit for NHSScotland organisations to undertake quarterly reporting against the standards
- National support provided by NHS Quality Improvement Scotland that takes into account self reporting by NHSBoards against the national standards
- Training modules in Information Governance for NHSScotland staff at certificate, diploma and Masters level
- An information portal on Information Governance to ensure staff have access to all the support materials needed to ensure good up to date practice[3] together with NHSScotland publication a '*Brief Guide to Information Governance*[4]' now available to all staff.
- Networks of key staff that meet regularly to review progress – this includes data protection officers; information governance leads; IT security officers; Caldicott Guardians; and records managers.

38. In addition a revised version of the Manual for Caldicott Guardians has been published and a Scottish version issued. The UK Council of Caldicott Guardians has also been established with representation from Scotland.

39. The National Information Governance Standards were based on the BSI 17799 requirements as is the NHS Scotland Information Security Policy document HDL (2006) 41[5]. These cover: Information Governance Policy and Planning; Confidentiality; Freedom of Information; Administrative Records; Patient Records; Data Protection; Caldicott Guardians; Data Quality; and Information Security.

40. Under the guidance of NHS QIS all NHS Boards have assessed their compliance with these standards; reported on the outcome; and prepared an action plan to address gaps in compliance.

Information Governance Educational Competency Framework

41. NHS Education for Scotland (NES) and the Information Governance Team have collaborated with representatives from Scottish Government and the NHS Boards to produce a new Information Governance Competency Framework to support the education and training of all NHS Scotland staff in this important area.

42. At the heart of the resource is a framework of competences describing effective Information Governance practice at four levels – ranging from Foundation to Advanced. This tool is designed to assist NHS Boards and other healthcare providers with the identification of education and training needs, and the planning,

[2] http://www.nhshealthquality.org/nhsqis/2762.html
[3] http://www.elib.scot.nhs.uk/portal/ig/Pages/index.aspx
[4] http://www.elib.scot.nhs.uk/SharedSpace/ig/Uploads/2007/Jun/20070608170750_V2%20Info
[5] http://www.sehd.scot.nhs.uk/mels/HDL2006_41.pdf

design and commissioning of training and development. The Framework is organised according to the HORUS (Holding, Obtaining, Recording, Using and Sharing information) principles and presented as discrete outcomes, enabling staff, managers and learning and development departments to use the competences flexibly in accordance with local needs. The Framework is also linked to relevant Knowledge and Skills Framework dimensions for staff covered by Agenda for Change.

Good Practice: Scottish Government

43. The Scottish Government's own centralised approach to information management and its accessible guidance and policies for information security led to a positive response in the questionnaire with all internal Scottish Government respondents aware of where accountability for data handling and management of risk sat within the organisation.

44. An Information Management Unit was set up in 2004 to promote good information management practices. The focus of the unit was in helping staff to do their job more efficiently and effectively and ensuring that the Scottish Government complied with its obligations under the various information rights legislation. Considerable work has been completed in assisting all Scottish Government staff to improve their understanding and consistency of approach to information management. The Scottish Government established 6 key principles for good information management that all staff must follow. In basic terms the principles are that:

- We treat information as a Scottish Government resource.
- We are all responsible for our information.
- We make information accessible to others who need to use it, in line with the law and best practice.
- We keep records of what we do.
- Our information is accurate and fit for purpose.
- Our information complies with regulations and legal requirements.

Key Recommendations

45. The Scottish Government itself holds substantial information on citizens and businesses. Government Departments elsewhere in the UK maintain a wide range of information systems themselves, each holding a significant number of records some of which relate to Scottish citizens and businesses. To deliver public services effectively and efficiently, information needs to be shared between different parts of Government. However, the public have a right to expect the information that they provide to Government will be held securely and used appropriately.

46. It is essential to retain public trust in Government's use of information. There must be visible and transparent measures in place to demonstrate that the personal data of citizens is treated with sensitivity, care and diligence – public servants must show by their actions as well as their words that they treat information about other people as carefully as they would treat their own. The recommendations below are intended to address the issues and concerns identified by this review and to build on

good practice across the wider public sector. The processes and procedures which will support these recommendations will continue to evolve in line with emerging technology and services. Information assurance will always be an ongoing process. The challenge to the Scottish Government is to foster a culture of continuous improvement in effective risk management while supporting service delivery and enabling legitimate information sharing. The key recommendations are that:

- The Scottish Government should provide leadership and act as the source of centralised, authoritative guidance and assistance for Scottish public bodies; for example by establishing overarching policies for information security, risk management and data sharing.

- The Scottish Government should be proactive in ensuring compliance with security standards, and actively monitor compliance through audits or health checks.

- The Scottish Government's expectations of public bodies on information security, risk management and data sharing must be clearly defined and easily accessible. In particular the rules and boundaries for data sharing should be explicit to ensure that there is no disparity between public sector bodies as regards their technical solutions, data handling procedures or working practices.

- The Scottish Government should ensure that policies and procedures do not impede legitimate access to information and data sharing in ways that either increase risks to citizens or are detrimental to efficiency.

47. The supporting recommendations fall into 3 major themes: Leadership and Governance, Process and Compliance, Communication and Culture

<u>Leadership and Governance</u>

48. A common theme emerging from the survey results and discussions with the wider public sector was the requirement for the Scottish Government to provide leadership and act as the source of centralised, authoritative guidance and assistance for Scottish public bodies on information risk management. This approach is consistent with the experience of NHS Scotland. The fact that there is a widely promulgated set of standards and processes within NHS Scotland has paid dividends; with a higher degree of understanding and consistency of approach to risk management.

49. The Scottish Government will provide the overall strategic direction for information assurance across the public sector in Scotland and will support and monitor the implementation of the recommendations within this report across central government. Progress in taking forward these recommendations will be overseen by the Scottish Government's Information Security Committee. The Scottish Government will support improvements across the wider public sector in Scotland, recognising different responsibilities and circumstances.

50. The proposed governance mechanisms include:

- Supplementing the existing Statement on Internal Control (SIC) with information assurance measures including the need to handle information accurately and securely and in completing the Statements on Internal Control the Accountable Officer will be supported by the written judgement of the information asset owners and the SIRO;
- Reinforcement of the Senior Information Risk Officer (SIRO) role through mandating aspects of their role and giving existing senior managers within organisations specific responsibility to improve the management mechanisms for data sets as "information asset owners"; and
- A formalised process for at least an annual assessment of information risk management.

Process and Compliance

51. Information is a key asset and its proper use is fundamental to the delivery of public services. The aim in introducing new processes and an enhanced compliance regime is to ensure that the management of information risk becomes part of standard performance monitoring. We intend to strike the right balance between enabling the appropriate use and sharing of data and ensuring that information assurance is still effective. The process measures which are being currently being introduced within the Scottish Government include:

- Identifying information assets and ensuring each has a named responsible owner;
- Application of an agreed cross government definition of the minimum personal data requiring protection;
- Application of a set minimum mandatory measures for the protection of information;
- Accountable Officers to cover information risks in their Statements on Internal Control from 2008 - 09 onwards;
- Completion of an annual assessment process to support the Accountable Officer's judgement in the Statement on Internal Control;
- Phased introduction, as new systems come on line, of greater access control to record access to and use of personal data;
- Introduction of Privacy Impact Assessments for major new projects which could have an impact on privacy. Privacy Impact Assessment is a tool which has been used successfully in other countries and which has been promoted recently by the Information Commissioner's Office. It is applied at the early planning stage in the life of a project to ensure that risks to privacy are properly assessed and managed;
- Revised approach to the access of personal data outwith secure premises and implementation of appropriate encryption mechanisms for laptops and data in transit;
- Updated guidance on the secure disposal of electronic and hard-copy media reviewed against latest government-wide best practice; and

- Establishment of an information assurance resource within the Scottish Government to increase the expert skills available to the wider public sector.

52. The compliance regime within the Scottish Government will include:

- Increased use of the accreditation process, developed to provide assurance for systems holding national security information, for systems holding personal data;
- Inclusion of information assurance within the Scottish Government's Gateway review process; and
- Assessment of the set of minimum standards through the Statements on Internal Control and audit process, backed up by spot checks by the Information Commissioner.

53. The Information Commissioner has for some time been pressing for powers to be pro-active in investigating compliance with the Data Protection Act and the Scottish Parliament passed a motion (S3M-1017) calling for such powers for the Assistant Information Commissioner for Scotland. This is a reserved matter and the UK Government announced that the Information Commissioner would be given authority to carry out spot checks to audit the security of the handling of personal data and the methods used when it is shared. The ICO intend to start 'spot check' audits when formal confirmation from the relevant UK Secretary of State is received. Independent scrutiny is important for promoting high standards of compliance and the Scottish Government will invite the Commissioner to make spot checks on the proper protection of personal data, consulting on how this can best be achieved within the resources available to the Commissioner.

54. These measures are being shared with the wider public sector. Agencies and NDPBs will be expected to make progress towards compliance in a reasonable timescale in consultation with the Scottish Government.

55. In addition we will be encouraging work on standards and procedures in the wider public sector. The review across the UK has indicated that the Information Commissioner will work with local government on identifying standards and good practice, in the same way that he has for central Government and that work is being initiated by the Local Government Association in England on new material and approaches. The Scottish Government will discuss with COSLA and the Assistant Commissioner for Scotland at the Information Commissioner's Office the mechanisms for ensuring that Scottish local government has the opportunity to be involved in similar developments.

56. The Scottish Government has kept in touch with the Cabinet Office on emerging findings, with a view to sharing best practice and identifying common approaches and processes for risk identification and management. The Scottish Government is adopting the new security standards and processes along with supporting technologies accredited by GCHQ for our internal systems.

57. We intend to revise the customary contract clauses used by Government to reflect the new standards. The Scottish Procurement Directorate will ensure that new contracts awarded by the Scottish Government reflect the appropriate changes.

Communication and Culture

58. These recommendations and processes are intended to raise the profile of information security within the public sector, increasing awareness of information security threats and risks, and publicising the standards and information available currently available. The aim is for the Scottish Government to create a public sector culture that values, uses and protects the data entrusted to it through:

- Working with colleagues and partner organisations across the public sector to make the existing guidance more user friendly and widely available;
- Supplementing existing guidance with a shorter set of core minimum requirements applicable to all central government; ensuring that communications clearly state that these are minimum measures and recognising that many public bodies will go beyond these measures;
- Investigating mechanisms to make risk management and data handling education more consistent and widely available;
- Reflecting the changes in HR processes, in particular emphasising responsibility for compliance with controls and standards; and
- Setting expectations that guidance and requirements will not remain static but will evolve and develop to keep pace with changing services and technologies, meaning that this is not a 'one off' exercise but rather a change in mind set across organisations.

59. A communications programme will be developed that recognises the need for the Scottish Government to communicate clearly to Agencies, NDPBs, and partner organisations exactly what their responsibilities are and what actions will be required of them to ensure they are properly prepared for these responsibilities. Communication on the work underway and the results of the changes in process will be shared not only with the wider public sector but with the public by:

- A commitment to publish material on information assurance in the Scottish Government annual report;
- Sharing information openly: continuing the principles the Scottish Government have established of being transparent about sharing information where that is to the genuine benefit of the individual and of the community, and sharing only that which is necessary to share for a particular purpose;
- Currently the DPA requires us, and all data controllers, to notify the Information Commissioner as to what personal data is used and for what purposes. This notification is published on the ICO's site but is not sufficiently detailed or explicit to allow citizens to easily understand what use we are making of their personal information and we will work to improve this; and
- The Scottish Government's published information asset register will be updated and enhanced in line with emerging good practice.

Implementation plan

60. Work is already underway to raise the awareness of information risk within the Scottish Government. All staff have been reminded of the need for appropriate care to be taken with data received, stored or transmitted to other bodies and of the tight security standards, including encryption and password protection as necessary, that already exist for the storage and transmission of data of a sensitive nature, in particular where this relates to personal information. These standards are continuing to evolve to reflect best practice in both government and industry and the seriousness with which the Scottish Government has always treated issues of data handling.

61. However, agreeing and putting in place these new arrangements across central government is a significant undertaking and work will continue over the next year. Progress in taking forward the recommendations of the report will be overseen by the Scottish Government's Information Security Committee.

- An exercise with the few low scoring organisations, to ascertain depth and breadth of issues, and identify further remedial action that should be taken to address problems will complete by the end of June 2008.
- A follow-up review will be carried out with those organisations that performed less well in the review and this will report back in September 2008.
- Additional work is already underway to better understand the gaps in information assurance that have been highlighted and an exercise planned to verify the baseline indicated by the responses in the exercise. This will complete by summer 2008.
- In addition a number of audits are planned to validate the accuracy of the responses from medium/high scoring organisations. These will be conducted on a cross section chosen at random and be completed by summer 2008.
- The organisation which used the questionnaire to request support for helping develop an information management policy has already been contacted and this exercise is now underway.
- Interest in the use of shared services that might allow data sharing and exchange with information held centrally and accessed over secure channels will be followed up with the specific organisations identified by summer 2008.
- Work has started on the addition of information assurance requirements to the Statement of Internal Control assurance checklist. These additions will be communicated as part of the revised checklist more generally with information risks included in the Statements on Internal Control from 2008 - 09 onwards and subject to audit process.
- We plan to set up periodic information security forums. These will enable sharing of guidance and standards on information security across the Scottish Public Sector and provide a mechanism to identify emerging good practice and improve awareness and accountability. We are also planning an annual forum for senior management on information assurance more generally.

Liaison across government

62. We remain in touch with colleagues across the wider public sector and the Scottish Government continues to participate in government-wide security initiatives, through our CIO, especially those focused on data security, privacy and strong user authentication.

63. The Central Sponsor for Information Assurance (CSIA), within the UK Government Cabinet Office, is responsible for providing strategic direction in information assurance, and guidance on the management of information; the Scottish Government has been working with the CSIA guidance for some time. Advice on the management of information risks is also available from the British Standards Institute in the ISO 27000 family of standards for information security management systems. These standards are published and were developed in close co-operation with experts in the Cabinet Office and CESG (the part of GCHQ that acts as the National Technical Authority for Information Assurance), to address the full range of information security policy and good practice. The ISO 27000 standards are reflected in a set of information security standards developed specifically for Government, and incorporated in the Government's Manual of Protective Security. This manual was first issued in 1994, was updated in August 2007 and is currently being revisited. The Scottish Government internally enforces the standards of Manual of Protective Security and promotes ISO 27000 standards across its Agencies and NDPBs.

64. Data protection is a reserved matter and the Scottish Government is bound by the Data Protection Act 1998 (DPA), updating previous legislation and implementing the 1995 European Directive on Data Protection. The DPA requires anybody processing personal information to comply with eight principles, one of which is to ensure that personal information is secure. The UK Government is committed in principle to the introduction of new sanctions under the DPA for the most serious breaches of its principles. Under the DPA, the Information Commissioner has a general duty to promote good practice by data controllers and in particular to promote the observance of the requirements of the Act by data controllers. In fulfilment of this, the Information Commissioner's Office (ICO) has published a series of guides designed to make data protection simpler, targeted at organisations and individuals alike.

Conclusion

65. Scotland has a strong commitment to safeguarding privacy and protecting the personal data of Scottish citizens. Indeed Scotland's performance in protecting privacy has been recognised by the international group Privacy International. In the 2007 Review of global privacy for the first time Scotland was given its own ranking score and performed significantly better than England and Wales.

66. Overall this review has found that data protection is being taken seriously across the Scottish Government and its agencies but that there is room for improvement. There is substantial good practice in Scotland but there have also been a few breaches of security, emphasising the importance of robust tracking procedures and proper encryption and password protection of sensitive personal

data which is stored on removable media or transmitted electronically between organisations. Smaller organisations with smaller holdings of data generally found it more difficult to devote adequate resources to delivering their data protection responsibilities than large organisations holding substantial quantities of data.

67. The assessment of review team was that there is a need for further measures to improve the security of sensitive information. In line with the conclusion of the earlier update and the stated views of the respondents to the questionnaire, we believe that there is a need to have higher levels of oversight and guidance – rather than these bodies fending for themselves and devising their own policies, procedures and guidance. This approach would also be consistent with the clear evidence from the returns that having a single and universally understood approach to information governance will pay dividends.

Annex A

Data Handling Exercise – Responses

Scottish Government

Permanent Secretary

Directors-General

DG Economy
DG Environment
DG Health
DG Justice& Communities
DG Education

Office of the Permanent Secretary

Non Ministerial Departments

General Register Office for Scotland
Office of the Scottish Charity Regulator
Registers of Scotland

Executive Agencies

Accountant In Bankruptcy
Crown Office and Procurator Fiscal Service
Fisheries Research Service
Historic Scotland
HM Inspectorate of Education
Mental Health Tribunal for Scotland
National Archives of Scotland
Scottish Courts Service
Scottish Fisheries Protection Agency
Scottish Prison Service
Scottish Public Pensions Agency
Scottish Work Inspection Agency
Student Awards Agency Scotland
Transport Scotland

Executive NDPBs

Accounts Commission for Scotland
Bord na Gaidhlig
Crofters' Commission
Cairngorms National Park Authority
Deer Commission for Scotland
Highlands & Islands Enterprise
Learning and Teaching Scotland
Loch Lomond & Trossachs National Park Authority

National Library of Scotland
National Museums of Scotland
Police Complaints Commission for Scotland
Risk Management Authority
Royal Botanic Garden Edinburgh
Royal Commission on the Ancient and Historical Monuments Of Scotland
Scottish Agricultural Wages Board
Scottish Children's Reporter Administration
Scottish Commission for the Regulation of Care
Scottish Criminal Cases Review Commission
Scottish Enterprise
Scottish Environmental Protection Agency
Scottish Further and Higher Education Funding Council
Scottish Legal Aid Board
Scottish Legal Services Ombudsman
Scottish Natural Heritage
Scottish Qualifications Authority
Scottish Screen
Scottish Social Services Council
Scottish University for Industry
Sportscotland
Visit Scotland
Water Industry Commission for Scotland

Advisory NDPBs

Architecture and Design Scotland
Building Standards Advisory Committee
Fisheries (Electricity) Committee
General Teaching Council for Scotland
Local Government Boundary Commission
Mobility and Access Committee for Scotland
Public Transport Users Committee for Scotland
Scottish Industrial Development Advisory Board
Scottish Law Commission
Scottish Local Authorities Remuneration Committee

NHS in Scotland

Golden Jubilee Hospital
NHS Quality Improvement Scotland
NHS National Services Scotland (includes the Scottish Advisory Committee on Distinction Awards)
Scottish Ambulance Service
Health Scotland
NHS 24
NHS Education for Scotland
The State Hospital
NHS Ayrshire and Arran
NHS Borders
NHS Dumfries and Galloway
NHS Fife
NHS Forth Valley
NHS Greater Glasgow and Clyde
NHS Grampian
NHS Highland
NHS Lanarkshire
NHS Lothian
NHS Orkney
NHS Shetland
NHS Tayside
NHS Western Isles
NHS Education for Scotland (NES)

Others

Highlands & Islands Airports Ltd
Mental Welfare Commission for Scotland
CalMac Ferries Ltd

Annex B

Minimum scope of Protected Personal Data

Public Bodies must identify data they or their delivery partners hold whose release or loss could cause harm or distress to individuals. This must include as a minimum all data falling into one or both categories below.

Category A: Any information that links one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress.

1. one or more of the pieces of information which can be used along with public domain information to identify an individual	**Combined with**	**2. information about that individual whose release is likely to cause harm or distress**
Name / addresses (home or business or both) / postcode / email / telephone numbers / driving licence number / date of birth [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]		Sensitive personal data as defined by s2 of the Data protection Act, including records relating to the criminal justice system, and group membership DNA or finger prints / bank, financial or credit card details / mother's maiden name / National Insurance number / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing

These are not exhaustive lists. Departments should determine whether other information they hold should be included in either category.

Category B. Any source of information about 1000 or more identifiable individuals, other than information sourced from the public domain.
This could be a database with 1000 or more entries containing facts mentioned in box 1, or an electronic folder or drive containing 1000 or more records about individuals. Again, this is a minimum standard. Information on smaller numbers of individuals may warrant protection because of the nature of the individuals, nature or source of the information, or extent of information.