

REPORT ON THE NORTHERN IRELAND DATA PROTECTION REVIEW

FEBRUARY 2008

BILL McCLUGGAGE

**CHIEF INFORMATION OFFICER
NORTHERN IRELAND CIVIL SERVICE**

Department of Finance & Personnel
Delivery & Innovation Division
Clare House
303 Airport Road West
BELFAST
BT3 9ED

TABLE OF CONTENTS

FOREWARD BY THE RT HON PETER ROBINSON MP MLA.....	5
BACKGROUND.....	7
SCOPE OF REVIEW	7
SELF-ASSESSMENT MECHANISM.....	8
RESPONSE LEVELS	9
NORTHERN IRELAND DATA PROTECTION REVIEW FINDINGS	10
OVERALL ASSESSMENT.....	10
AREAS OF GOOD PRACTICE.....	10
AREAS IDENTIFIED AS REQUIRING IMPROVEMENT	10
RECOMMENDED ACTIONS.....	11
ACTIONS TAKEN TO DATE.....	13
CONCLUSION.....	15
GLOSSARY.....	16

REPORT ON THE NORTHERN IRELAND DATA PROTECTION REVIEW

FOREWARD BY THE RT HON PETER ROBINSON MP MLA

When I announced my Data Protection Review in November 2007, it was against the backdrop of a series of data security incidents across a number of UK Government Departments. I wanted to assess the effectiveness of data protection measures in place in Northern Ireland, to establish that appropriate and proper systems of data protection and control were in place and functioning properly.

The completed review has highlighted a number of specific areas of good practice operating across Departments and Agencies, particularly in the fields of fraud detection, security and access and connectivity. However, it also revealed a range of areas where organisations recognised that there was scope for significant and urgent improvement – such as training, information transfer and risk management - and identified a clear need for us to match the rapid change in the technology landscape by updating our policies and procedures.

In light of these Review findings, Departments, Agencies and Non-Departmental Public Bodies are now implementing changes which will help them keep a sharp focus on data protection and related issues. I am particularly pleased that a range of actions to improve awareness, audit and encryption activities have already commenced and Departments have started to make significant progress on their respective Action Plans. Further re-assessment of data protection capabilities will take place by the end of April 2008 to confirm actions have been implemented and reaffirm that the requisite level of protection measures are in place.

We all recognise that custodianship of personal information is an extremely important matter and I want to ensure, as will my Ministerial colleagues, that all such information is properly safeguarded when in the care of public sector organizations across Northern Ireland. I welcome the forthright and open manner in which organisations responded and the follow-up actions identified by the review will assure that our Devolved Administration in Northern Ireland

maintains the highest level of good practice in all areas where it has a duty of care for personal data entrusted to us by the public.

BACKGROUND

The Northern Ireland Data Protection Review was commissioned by the Minister for Finance & Personnel, the Rt Hon Peter Robinson MP MLA on 21 November 2007 following a series of personal data security incidents across a number of UK Government Departments.

The Review was led by Bill McCluggage, the Chief Information Officer (CIO) for the Northern Ireland Civil Service together with a small project team, with the purpose of:

- Defining areas of good practice (capability drivers);
- Using capability drivers to self-assess the areas of Management, Operational and Technical capability across NICS Departments, Agencies and Non-Departmental Public Bodies;
- Identifying specific areas of good practice and areas requiring attention across the range of capabilities; and
- Listing a generic set of recommendations to address identified areas of weakness.

SCOPE OF REVIEW

The Review studied all 11 NICS Departments together with 57 Agencies and NDPBs. Local Authorities and the Voluntary & Community sectors were not included.

The primary focus of the study was on the policies, procedures and behaviours driving Management, Operational and, to a lesser degree, Technical capabilities defining the intra-organisational, inter-organisational and external exchange of personalized data. Taking the form of a self-assessment questionnaire, each organisation was asked to consider and assess their position against a capability model covering each of the three drivers.

The Information Commissioner in Northern Ireland was briefed on the scope of the Review and provided valuable assistance and advice prior to the assessment being carried out.

In addition, the Department of Social Development also undertook their own specific assessment exercise which was separate from, but fed into, this review.

SELF-ASSESSMENT MECHANISM

The project team designed a specific and detailed capability maturity model compiled from a range of best practice guidelines. The assessment questionnaire was accompanied by a comprehensive set of guidelines on how to assess capabilities covered in each area.

The capability model was based upon four levels of maturity, these being:-

Ad hoc (lowest level): there is limited or no policies, procedures or controls in place;

Defined: controls are mostly documented although all staff may not be aware or trained on the policies and procedures or where adherence may be patchy;

Managed: formal documented policies and procedures are in place, supported by well-designed practices which generally operate effectively;

Optimised (highest level): formal documented policies and procedures are in place and are supported by well designed and successfully implemented working practices which operate effectively, are monitored routinely and are independently assured.

These four self-scored levels of maturity were then interpreted by the project team to provide an overall assessment of data protection capability for the Northern Ireland Departments, Agencies and NDPBs.

RESPONSE LEVELS

The Review was carried out over a four-week time span in late November and December 2007 and received a total of 68 returns for analysis.

This was considered to be a sufficiently representative level of response by organizations across which to assess the overall level of data protection maturity levels and capabilities.

NORTHERN IRELAND DATA PROTECTION REVIEW FINDINGS

OVERALL ASSESSMENT

Given the detailed level of assessment and an analysis of the returns supplied by Departments, Agencies and NDPBs, the review team concluded that the overall capability of the assessed organisations met an overall maturity of 72%.

However, the returns also indicated that there is a clear need for improvement and appropriate urgent remedial action in six key areas. These are highlighted in the section entitled 'Areas Identified as Requiring Improvement' below.

AREAS OF GOOD PRACTICE

The Review highlighted a number of areas of good practice. These were based on assessed returns at Managed level or higher as follows:-:

- Prevention and detection of fraud (83%);
- Security of interconnects (78%);
- Physical and environmental management (80%);
- Handling complaints and incidents (82%); and
- Physical security and access (78%).

AREAS IDENTIFIED AS REQUIRING IMPROVEMENT

The Review also indicated that several key drivers that underpin excellent levels of data protection maturity were open for improvement. This analysis was based on returns highlighting either an Ad hoc or Defined level as follows:-:

- Awareness and training (53%);
- Use and protection of media (53%);
- Management of configuration changes (50%);
- Business continuity (38%);

- Outsourced technical competencies (35%); and
- Information transfer and communication (31%).

RECOMMENDED ACTIONS

In order to support the necessary rapid improvement in those areas identified for urgent action, during the intervening period between the delivery of the draft findings and this report, a corporate Action Plan has been developed and is in the process of being implemented to further strengthen and develop data protection measures across Departments, Agencies and NDPBs.

First and foremost, all organisations have been asked to define and implement an Action Plan to strengthen governance and compliance policies and procedures within a 90 day period, with the objective of placing themselves into at least a well managed data protection environment.

By implementing the required levels highlighted in these Action Plans, the Review Team consider that organisations should be well placed during any further self assessment exercise to fully meet best practice guidelines.

Additionally, all participating organisations have been asked to consider:-

- A review and improvement of governance arrangements with Board level visibility;
- Awareness and training (annual refresher training should emphasis on a case-by case basis the likely impact from a citizen's perspective of a breach of data protection protocols) ;
- The use of protected media (review each instance of data transfer involving hard media to ensure appropriate levels of password protection and encryption are employed);

- Configuration management (all changes to systems should be assessed in terms of their ability to jeopardise the control of personal data);
- The transfer of information across system boundaries including identifying and mapping data conduits and assessing the correct types and volumes of data to be transferred;
- Improvement to risk management techniques, including:
 - 6 monthly Governance reviews;
 - Establishment of risk registers with visibility at Board level;
 - Responsibilities under DPA should be included across all Internal Audits;
- Initiating actions to introduce mandatory encryption and password protection for laptops/PCs/USB and other removable data storage devices;
- A further self assessment to ensure that data protection capability has reached a sufficiently robust level within their organisation.

Additionally, the Department of Finance & Personnel also agreed in December 2007 to drive forward further development of data protection capabilities across Departments, Agencies and NDPBs by:-

- developing a training template for the NI Departments, Agencies NDPBs based upon guidance from the ICO ;
- developing an NI public sector DPA awareness campaign (similar to recent FOI campaign);
- developing guidance on the requirement for the protection of electronic media across NI Departments, Agencies & NDPBs;

- drafting a citizens charter to reflect an agreement between government and the citizen on the effective custodianship of personal data;
- developing a Northern Ireland Code of Practice for Information Sharing;
- developing guidance on the assessment of supplier data protection capability;
- recommending that data protection principles be embedded as a key indicator within best practice accreditation (IIP/ Chartermark / EFQM); and
- reviewing progress of organisations against their 90-day NI Data Protection Review improvement programmes.

ACTIONS TAKEN TO DATE

- (a) We have identified a suitable delivery mechanism for a DPA training toolset, identified the supplier and initiated delivery of the first product which will be a short data awareness eLearning package for induction and immediate refresher training on critical aspects of DPA;
- (b) We have initiated the delivery of a DPA awareness campaign for Departments, Agencies, Non-Departmental Public Bodies and wider public sector in Northern Ireland which will run from May-October 2008;
- (c) We have agreed with the Chief Executive's Forum (CEF) to run an awareness seminar as soon as possible;
- (d) Work has been initiated on the development of a Citizen Charter on the handling of personal data and a Code of Practice for information sharing;
- (e) We are in the process of drafting a note to the Northern Ireland Audit Office inviting it to include relevant aspects of data protection within their routine audit activities;

- (f) As far as laptop security is concerned, and following the laptop policy directive from Sir Nigel Hamilton to the NICS, a revised policy on the use of laptops and removable storage media will issue in February 2008;
- (g) Procurement of an accelerated laptop refresh programme has been initiated and this will result in the availability of the requisite approved encryption capability by the end of March 2008. In the interim, and following the directive from Sir Nigel Hamilton, we have issued amplified guidance on the risk management approach to be employed with laptops and removable storage media which leave secured premises;
- (h) In order to unblock current constraints on the day-to-day transfer of personal data files between organisations connected to the Government Secure Intranet (GSI) we await the clearance by HMRC/DWP/CESG of a capability to use the GSI as a preferred secure transfer route. We are aware that an appropriate product has been developed by Cable and Wireless, the GSI supplier, which is currently being evaluated and we hope this will be cleared imminently;
- (i) In addition, we are currently procuring a secure file transfer capability using a rapid procurement route agree with our Central procurement Directorate through the Office of Government Commerce (OGC) eTransaction framework. This service should be available to Northern Ireland-wide public sector organisations that are not connected to the GSI (including the majority of NDPBs) by early March 2008.

CONCLUSION

The Minister for Finance & Personnel instigated a review of the capability of the Northern Ireland Departments, Agencies and NDPBS to assess the effectiveness of their data protection measures.

The review team noted that there were a range of areas of good practice although they also observed that there were a significant number of areas where urgent action was required.

It is also acknowledged that the introduction of new technology will not in itself provide the requisite levels of improvement. Only by adopting a more holistic approach involving changes to behavioural, procedural and technical capability will the requisite levels of data protection maturity be achieved.

However, organisations have already adopted a more proactive approach to the delivery of data protection within their business areas. All of the organisations who took part in the self-assessment exercise did so proactively, openly and in a totally professional manner. Nonetheless, if Northern Ireland Departments, Agencies and NDPBs are to assure the public that they provide the highest level of data protection, they must continue to focus on achieving an exemplary level of awareness, behaviours and technical procedures.

The review team consulted with the Information Commissioner for Northern Ireland during the review process and on the findings of the review. She was very supportive and provided additional valuable input.

Hence, given the actions that are currently underway, it is anticipated that over the next 90 days, the NI public service will be much better placed to meet the challenges imposed by a growingly complex and modern data protection environment.

GLOSSARY

CEF	Chief Executive's Forum
CIO	Chief Information Officer
DPA	Data Protection Act
EFQM	European Foundation for Quality Management
FOI	Freedom of Information
ICO	Information Commissioner's Office
NDPB	Non-Departmental Public Body
NICS	Northern Ireland Civil Service