An Coimisinéir
Cosanta Sonraí

Data Protection
Commissioner

Data Protection in the Department of Social & Family Affairs

Report by the Data Protection Commissioner

Table of Contents

Executive Summary…………………………………………………………....P.3

1 **Legal Basis for Inspection**………………………………………………..P.4

2 **Background**……………………………………………………………….P.4

3 **Pre-Inspection**……………………………………………………………P.6

4 **The Inspection**……………………………………………………………P.7

4.1 Technical Infrastructure………………………………………….P.7

4.2 Data Protection Policies & Practices……..…………………….P.10

4.3 Inspection of Specific Divisions & Systems…………………P.14
4.3.1 Illness Benefit……………………………………...…P.14
4.3.2 Statistics Unit…………………………………………P.15
4.3.3 ACMS Child Benefit……………………………….……P.16
4.3.4 Medical Certs…………………………………………P.16
4.3.5 ISTS (Integrated Short Term Systems)………………P.17
4.3.6 Client Identity Services……………………………….P.18
4.3.7 Control Division – Regional Directors Office………..P.21
4.3.8 Public Office (Oisín House)……………………………P.22

4.4 Third Party Data Feeds…………………………………………..P.22

4.5 Additional Findings relation to IT Operations Group………...P.23

5 **Findings**…………………………………………………………………....P.24

6 **Recommendations**………………………………………………………...P.27

7 **Review of Progress**……………………………………………………..P.32

8 **Appendices**………………………………………………………………...P.32

Throughout this report, the abbreviation "DSFA" stands for "Department of Social and Family Affairs" and the abbreviation "ODPC" stands for "Office of the Data Protection Commissioner"

EXECUTIVE SUMMARY

This is a report of an audit of the Department of Social and Family Affairs carried out by the Office of the Data Protection Commissioner in January of this year. The Department fully cooperated with the audit.

The Department was selected for audit in the light of its status as a major holder of personal data on individuals. Much of this data is provided in circumstances where the individual has no choice but to give the information if they wish to receive a service or benefit.

The audit took place against a background of significant concerns in relation to the data protection practices in the Department. These concerns arose from audits of other organisations such as insurance companies, complaints to the Commissioner and media reports of illegal leaks of information.

The report highlights specific issues of concern and a large number of areas where improvement is necessary. The need for such improvement is fully acknowledged by the Department.

The Department is devoting more resources and senior management attention to data protection. It is embarked on a programme of change in its practices which should lead to an increased level of compliance with data protection requirements. The Commissioner will continue to work closely with the Department to ensure that this progress is maintained.

1. LEGAL BASIS FOR INSPECTION

Section 10(1A) of the Data Protection Acts 1988 & 2003 states that

"The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and to identify any contravention thereof".

Under this authority the Commissioner instructed that an on-site inspection of the Department of Social & Family Affairs (DSFA) be conducted on 22-23 January 2008. An inspection team was selected consisting of Gary Davis, Deputy Commissioner, Eunice Delaney, Assistant Commissioner, John Rogers, Senior Compliance Officer, Ciara O'Sullivan, Senior Compliance Officer & Alan O'Grady, Senior Compliance Officer. Two additional resources, from a private sector technology company were temporarily designated as 'authorised officers' by the Commissioner for the purposes of providing technical assistance and expertise to the Team for the duration of the audit. Authorised officers have rights of access to personal data under Section 24 of the Acts with corresponding obligations of confidentiality. For the purposes of the audit the team sub-divided into business audit and technical audit teams. The letter of intention to audit issued by the Commissioner is attached at Appendix 1.

The main focus of audit activity is to identify improvements that may be needed to ensure that the requirements of the Data Protection Acts are fully observed at all times. In tandem with this objective, an audit is also designed to ascertain whether there are any discernible breaches of data protection requirements evident.

2. BACKGROUND

The quality of data security and access methods to personal data within Government Departments and bodies generally and particularly in the Department of Social & Family Affairs has been an issue of concern for a period of time.

Because of the nature of its work, the Department of Social and Family Affairs holds extensive and detailed personal information about its customers. It accepts that it has a responsibility to ensure that this information is collected appropriately, is maintained securely and is to be used only for the purpose for which it was intended. The Department takes these responsibilities seriously and considers breaches of data protection to be an offence warranting the highest disciplinary sanction.

The Department acknowledges and shares the public concern that there have been a number of breaches of data security in recent years and, in light of these events, has been engaged in a significant review of data access management and control policies , practices and procedures. The review, while not yet complete, has highlighted a number of weaknesses that the Department is committed to addressing in order to ensure that information security is enhanced to a level commensurate with the high level of importance attached to it by top management. In January 2008, the Department adopted a broad policy framework based on the principles that access to data will be on a 'need-to-know' basis, can only be accessed by authorised individuals and for the purpose intended, and that individual accountability will be ensured. It recognises that existing control measures do not fully comply with some of these requirements, but has indicated it is actively engaged in a programme of work to address the deficiencies.

It has stressed that many of the current weaknesses relate to the technological limitations of a number of the computer systems that support its customer schemes and services. These systems are commonly referred to as ‘legacy’ systems. When these systems were originally built, it was standard practice to make them available to as many business users as possible and to audit only changes to data. It has become apparent over the last number of years that these systems do not facilitate the requirements to limit access on a ‘need to know’ basis and to audit read-only access. As part of its Modernisation Action Plan and new Service Delivery Model, the Department is currently engaged in a multi-year programme to replace these applications and is moving to a platform that includes enhanced information security controls. The design of the Department’s new systems (known as the Business Object Model) includes, inter alia, better access controls and audit facilities. The Department has stated that it will replace/migrate all of its remaining ‘legacy’ systems over the next 5 years or so. The Department further states that the speed of migration is governed by the availability of resources in both the technical and business areas of the Department (who have to continue to operate and maintain current production systems while re-engineering Departmental processes and systems) but the Department recognises the desirability, on many grounds, of completing the migration as quickly as possible. In view of the criticality of its main client record system, it completed ‘retro-fitting’ a ‘read audit’ capability shortly after the Audit Team’s on-site inspection.

The discovery, during the course of an audit of an insurance company by the Office of the Data Protection Commissioner (ODPC) in June 2007, that the social welfare details of a number of individuals were held on the files of private investigators working for the company was accepted as a matter of deep concern by the Department. At that time, the ODPC wrote to the Department to request that the matter be investigated and safeguards reviewed to avoid recurrence. The Department is anxious to highlight that it takes its responsibilities in this regard very seriously and has been liaising with the ODPC in relation to this investigation.

The Department was scheduled for priority audit in direct response to further media reports in October 2007 alleging a series of unlawful disclosures of personal data by an employee of the Department who then used the information for criminal purposes (although it is noted that this case relates to events that took place in 2003 and that the official concerned was dismissed from the Civil Service). These incidents demonstrate the important human aspect of information security. While the Department has been engaged in a staff training and awareness programme for some time, it recognised, at the outset of the Audit, the need to enhance and expand the programme to better ensure that all of its 4,500 employees are provided with the knowledge, skills, tools and supports necessary to carry out their duties in a security-conscious manner.

Data Holding & Personal Public Service Number (PPSN)
DSFA is the largest holder of personal data on us all in the State. Collection of our personal data starts in the public sector from the moment we are born. Today, everyone is assigned a Personal Public Service Number (PPSN) at birth by DSFA. The Department holds personal data across the full spectrum of society. It holds personal data to pay, inter alia, child benefit, bereavement grants, old age pensions, maternity benefits, widow's/widower's pensions, lone parent scheme, carers allowance, jobseeker's allowances, back to work schemes, illness & disability benefits, rent allowance, free schemes such as free travel, TV licences, bottled gas, electricity, telephone and to take PRSI contributions.

This entails the holding of a full record of all of its customers' details including in many instances bank account details to facilitate the payment of benefits.

The PPSN was introduced in the 1998 Social Welfare Act as the unique personal identifier for transactions between individuals and Government Departments and other agencies specified in the Social Welfare Acts. Legislation regulating the use of the PPSN provides that it can be used either by the public bodies named in the Social Welfare Acts or by any person or body authorised by those public bodies to act on their behalf. While only specified public bodies can use the PPSN, equally it can only be used by such bodies for particular transactions and where the transaction relates to a public function of that body.

A person's related "public service identity" - the PPSN plus name (and any former surname), date of birth, mother's former surname, sex, nationality and address - is retained on a database in DSFA. Recent changes to social welfare law provided for the addition of signatures and photographs. This information may be shared with other agencies providing public services, subject to conditions laid down in the Social Welfare Acts.

The PPSN – originally the Revenue and Social Insurance Number (RSI) confined to transactions with the Department of Social and Family Affairs and the Revenue Commissioners – is today increasingly demanded by public agencies as a condition for providing a wide range of services.

<u>3. PRE-INSEPCTION</u>

The Commissioner wrote to the Department on 30th October 2007 formally notifying the Secretary-General of his intention to conduct an audit on a date to be agreed mutually. Advance documentation was also sought in relation to data flows and system architecture within the Department.

The audit was stated to focus on two main clusters of issues:

(i) The measures in place to protect the security of the personal data of customers of the Department of Social and Family Affairs.

(ii) Establishing a clearer picture of the extent of data-sharing in the broader public service using the PPSN as an identifier.

At the Department's instigation a pre-audit meeting was held on 14 January 2008 to allow for the audit to be conducted on the key areas of concern and in an efficient a manner as possible.

4. THE INSPECTION

The on-site inspection process was conducted over two days and sought to concentrate on those areas of activity of the Department which were considered by the ODPC to be likely to be indicative of the broader policies and practices in relation to data protection within the Department. By its very nature a two day inspection of a Department processing such an extensive amount of personal data in relation to the population cannot be considered to be exhaustive and the conclusions drawn and recommendations made should be viewed in that context.

The areas and operating systems of the Department selected for inspection were chosen at random, albeit, with a particular focus on those areas which were believed would be most illustrative of the physical and technical measures in place for the processing of personal data in the Department.

4.1 Technical Infrastructure

There are over 50 live systems within the Department which contain some elements of the personal data of customers and staff members of the Department. The principal system is the Central Records System (CRS) which held 6,817,262 client records at the end of November 2007. It is the central database for holding customer records. Query access to this system and all other systems is generally managed through what is known as the INFOSYS system. Direct access to individual systems is also possible. The CRS and INFOSYS systems are termed as legacy systems within the Department and are intended to be incorporated on a phased basis into the new Business Object Model (BOM) system as part of the Department's modernisation process.

CRS

Access to the CRS system is controlled by means of user accounts. A user account is set up on foot of an application from the user's business manager who determines what level of access is required for a given employee to perform their job role. This information is then given to the 'Data Access Control' group, based in Carrick–on-Shannon, who authorise the level of access to be given to the user within the CRS system and liaise with IT operations to set-up the new user.

The process is well-known within the Department, although no formalised documented procedure in this regard was available during the course of the inspection. The process by which users are removed from the CRS system (leaving, maternity, retirement etc.) was much less clear. There is no single documented procedure by which a user will be removed from a given system, including CRS. Access to the CRS is dictated by a user access system. If this account is removed or disabled, access to all other systems, including CRS, will also be removed.

DSFA are moving towards what is termed an Active Directory system which assigns access privileges to systems based on specific roles which will provide for a centralised mechanism to deal with users who leave. The Department has highlighted that it has carried out considerable work on Active Directory and this will facilitate the centralised and policy driven treatment of 'leavers'. It has stated that there is a considerable amount of work involved in defining Department wide roles and ensuring that the fact of a member of staff leaving is registered. The Department has confirmed that this work is underway and will continue.

The CRS system has a comprehensive logging and auditing capability whereby all updates, changes, additions, modifications, etc., to a CRS record are recorded and subsequently archived for future retrieval if required. The system did have a weakness in this respect which was well recognised by the Department at the time of the inspection. Specific development work took place by the Department in this respect which was implemented by the end of February 2008.

INFOSYS

INFOSYS is a 'read only' search facility that allows users query various DSFA databases. User access is assigned similar to the CRS system, with querying limited to the level of access indicated for the user by their business manager. As with CRS, there is no clear formalised documented procedure in place to ensure users that no longer require access are removed from the system. However, all activity through INFOSYS is logged and a complete audit trail of all 'look-ups' is retrievable.

There are a large number of external agencies who have access to INFOSYS. A listing provided by the Department is attached at Appendix 2. In this respect it was noted that there are a number of generic accounts and passwords on the system to allow access. These accounts can only be attributed to a particular area – and not to a specific individual. As such it would not be possible to provide a meaningful audit trail when such accounts are used. The Department highlighted that there has been a systematic programme of removal of such accounts and this will continue. In carrying this out, the Department has indicated that it must proceed carefully with regard to the fact that such accounts are used to deliver its customer services and alternative service options must be in place before accounts are closed down. Since the time of the audit all generic access to the INFOSYS and CRS systems have now been removed within the Department. Work is continuing to terminate what the Department views as the small number of generic accounts in use by external bodies. The ODPC has been assured that this work has a high priority for the Department.

Business Object Model Applications

It is planned that all DSFA legacy systems will be replaced by a single integrated software system with facilities for much more fine-grained control of access based on role. There is a ten year plan in operation to have all databases redesigned. The Department has indicated that there is no set timeframe for migration of all applications to the Business Object Model (BOM). However, it does fully recognise that it should take place as soon as possible while ensuring continuity of service delivery. The Department has pointed out that the timescale is primarily due to the fact that it is effectively operating two production environments with less resources than some years ago, while also changing and modernising its skill sets. The other reason put forward for the lack of a defined timescale is that the BOM is an integrated environment and its development has to take into account the interdependencies between systems and the particular business priorities at any time.

Databases created for SDM are built using what is termed Naked Object Architecture. Data held for a particular business object, e.g. Customer, is accessed through facilities provided by the object in question. In this instance users have access to a particular customer record but may receive different amounts of data depending on their agreed requirements.

User access is based on a component of the BOM called "Officer Object" which dictates access to the system on a business needs criteria.

Logging and Auditing is comprehensive throughout the BOM environment. Logging takes place at 'read' level and above, and all log files are archived to a secure archive database.

The system also incorporates a quality control checking system. Every significant action (defined as 'read' and above) in the system is recorded as a separate action. A proportion of those actions are randomly selected and flagged for quality control. They are designated to a particular officer who will review and sign off on them using digital certificates. Digital certificates are used extensively throughout the BOM providing a high degree of security.

The audit team was of the view that there was no obvious uniform methodology used for software development in the BOM environment. The Team noted this could lead to the use of non-standard coding practices, thus increasing the likelihood of introducing security vulnerabilities (bugs) into the system over time. This would then become increasingly critical as the BOM environment moves towards a web based model. The Department in response has highlighted that software development follows what is termed the 'Agile' approach and that this approach is evolving in a consistent fashion within the Department.

A number of systems have already moved to the BOM. The movement of the remaining systems to the BOM framework is to be recommended as soon as possible as it would seem to provide the appropriate systems for the processing of personal data. This is a point that is recognised by the Department. As stated above it has highlighted that it is maintaining two production environments and is engaged in a process of changing its internal skill sets. While it is building its capability, it has set up a framework agreement within which a number of external System Integrators are migrating its systems. It has emphasised that it must do this in a responsible and cost effective fashion while safeguarding existing services and in a way that allows it to maintain these systems into the future. An issue that also requires attention in this respect is the necessity once data has moved to remove access to older legacy systems. This does not seem to have occurred in relation to at least one system that has moved to the BOM so far. The view of the ODPC is that business users need to fully justify any such requirement to keep systems operating in the legacy mode. The Department has indicated that it does recognise that retirement of these systems is highly desirable as soon as business requirements permit.

4.2 Data Protection Policies & Practices

Business Information Security Unit (BISU)

The Unit was established in 2004 and is now part of the Department's Risk Management Division. It does, however, pre-date the Risk Management Division as a result of work commissioned by the Department under a review of its Information Security Architecture.

The BISU has Department-wide responsibility for developing, co-ordinating and promoting information security in the Department. Its role is to provide professional security services that enable the business to understand and manage information risk. The role of Head of Information Security is assigned to a Principal Officer drawn from within the Risk Management Division who reports to the Divisional Director. The Team were informed that the unit was focused on adopting three primary measures to address the security of information within the Department: "develop, co-ordinate and promote". It was outlined to the Team that historically there had been a fragmented approach in terms of information security policies within the Department until the establishment of BISU. Prior to the establishment of the BISU, responsibility for the disparate elements of information security was spread among a number of business and support units and co-ordinated at a senior level by a Business Information Protection Committee. The Committee comprised senior managers from all relevant business and support areas and was chaired by the Assistant Secretary with responsibility for Personnel. The post of Head of Information Security and the BISU were established as part of the new Information Security Architecture governance structures. In a further move towards consolidation, the data protection function was recently moved from within the remit of the Client Identity Services Unit and incorporated into the BISU area of responsibility.

The Department has indicated that since 2003, it has engaged in a broad programme of work to progressively implement a new Information Security Architecture. This it is stated provides a framework to support the design, implementation and maintenance of information security in the Department. In 2005, the Department engaged consultants to support an information Risk Management (iRM) project with a view to further embedding the process of managing information risk within the Department. This project is seen as a key component of the Department's overall Risk Management Programme in which the Department aims to drive down the potential damage arising from a loss of confidentiality, availability or integrity of its critical information resources. The Team was informed that this involved a risk assessment of 16 principal applications with a view to the development of a framework towards improved information security management. The recommendation that the Department should put in place a broad information security programme to address the weaknesses identified over a to 3 to 5 year period was highlighted as a key outcome from the commission of this independent external report (published in July 2006). The consultants acknowledged that this timeframe assumed that there would be no resource constraints which would preclude the time being devoted to individual projects or the running of multiple projects at the same time. They also agreed that it would be appropriate for cost and efficiency purposes to engage in an analysis of the extent to which existing or planned projects would address the risks identified before a definitive work plan was drawn-up.

While the Audit Team did not view the independent external report in question, the Department indicated that it has been progressively implementing the recommendations, including revised governance arrangements, the adoption of a policy framework, improved staff awareness, undertaking an internal penetration test and a range of IT security projects.

The Department has highlighted the following projects, which have a data protection element and which form part of the wider information Risk Management (iRM) 3-5 Year Works Programme which are proceeding in 2008:-

- Development of an Identity and Access Management Framework (the high-level policy approved Jan 2008 provides the context for a broad programme of work);
- Develop user access management procedures and processes for all business critical applications (A Data Access Control Policy set was approved in Jan 2008, and work is ongoing in relation to the development of procedures and processes required to implement policy and monitor compliance);
- Develop a set of Information Security standards and guidelines (ongoing 2008);
- Further develop and undertake Department-wide security awareness training (ongoing throughout 2008);
- Define and develop Info. Security, MIS and Reporting requirements (to commence Q3/2008);
- Development of an Information Security Classification Model;
- Conduct regular risk assessments of business critical applications;
- Penetration testing;
- Improved Network Device security controls.

The Department indicated that future requirements have not yet been fully quantified and will, inter alia, be influenced by the recommendations of this Audit.

The Audit Team was also informed of a High Level Data Access and Management Review Group. This group has a membership consisting of the Department's Personnel Officer, Director of ICT and the Director of the Risk Management Division. This development is seen as important in implementing a streamlined process towards progressing work plans and addressing any weaknesses within current systems. This Group is intended to operate as long as a need is seen for it to do so.

The Team was also informed of the existence of a High Level 'Risk and Operations Committee' (ROC) within the Department in which data protection had featured as a standing item on its monthly agenda. Data Protection is also currently a standing item on Management Board Meeting agendas.

Staff Training

IT staff and officers from within the Department are members of the *Information Security Forum,* a recognised international independent authority on information security. System Developers must complete a personal data security awareness programme as part of their training.

The Team was advised that since the issues re-emerged in relation to unauthorised disclosure in 2007, an enhanced staff awareness programme has been rolled-out. A data protection module now forms part of the induction course for all new entrants and a half-day standalone data protection course is being rolled out to regional DSFA offices. The Team noted this programme and highlighted practice in other organisations in terms of targeting the current cadre of staff also in addition to new entrants. On this basis, the Audit Team outlined practice in parts of the private sector such as an annual online completion of a training module on data protection. The Team also referred to a large private sector organisation which had incorporated data protection training as part of all its offsite intensive training programmes.

The Department has highlighted that since its inception in 2004, the BISU has been actively engaged in promoting staff awareness on information security through a broad programme using a variety of media. With regard to the formal presentations, there had been a focus on new entrants and line management induction, but this has been expanded to include Information Officers and outdoor staff (e.g. recent presentation on data protection given to 150 officers). The programme also includes regular online messages and reminders, articles in Departmental magazines, and office notices. The Department is currently reviewing the information security awareness strategy with a view to assessing how it could be further enhanced and welcomes the suggestions of the Audit Team in that regard.

Copies of data protection guidelines and policies as well as existing baseline security standards were provided to the Team.

The full-time resources dedicated to the BISU consist of the following: 1 Assistant Principal /3 Higher Executive Officers/1 Executive Officer. A consultancy budget of €500,000 has been allocated in 2008 to fund a range of information security projects which are seen as the most immediate and pressing elements of the Works Programme outlined above.

Data Breaches/Disclosures and Planned Actions to Improve Controls

It was indicated to the Team that that there have been seven alleged reported breaches since July 2007 which were brought to their attention. A new complaints reporting structure has been in operation commencing in the last quarter of 2007 and will be subject to a preliminary review shortly. All breach allegations are now channelled through the BISU for further investigation. At the time of the audit it was indicated that the BISU examines the ‘access log’ for the file of the customer in question. An ‘access log’ is typically a record of all queries, edits or updates made on an organisation’s systems by an individual using a particular username and password. Unusual access trends/patterns are examined and where necessary, the file is sent on for further investigation internally including, where appropriate, Human Resources Division which may chose to interview any employee whose pattern of access gives rise to concern and decide if/what disciplinary action is required on a case-by-case basis.

The Department has indicated that revised procedures were introduced with effect from April 2008, as follows: All complaints of a breach of data protection are forwarded to and recorded by the BISU. The BISU forward the complaint to the Internal Control Support Unit (ICSU), which is part of the Regional Director’s Office

(RDO), for investigation. The ICSU has a Department-wide brief in respect of the investigation of alleged breaches of data protection. The ICSU request ‘access logs’ relating to the customer record in question. Unusual access trends / patterns are examined and investigated as appropriate. If a breach of confidential customer data is established, the matter is referred to Human Resources for consideration of disciplinary action (under the Department’s Disciplinary Code) up to and including possible dismissal. The BISU is notified and maintains a central record of the outcomes of all investigations.

Regional Director’s Office – Internal Control Support Unit (ICSU)

The Internal Control Support Unit (ICSU) was established in 2006. Its main functions are to examine, monitor and report on internal control practices and procedures within the Local/Branch Office network; to provide advice and support on matters pertaining to internal control and to investigate cases of suspected fraud and or possible breaches of data security. There was a lack of clarity at the time of the audit as to how far this investigative ambit extended with some perspectives that it only related to unauthorised access in regional locations and not Head Office. As outlined above by the Department this position has now been clarified.

The primary role of the ICSU is in relation to dealing with fraud and robust systems were noted to be in place in this respect. In addition to an internal departmental fraud investigation unit set up two years ago by Risk Management Division, the Department operates regional fraud investigation teams that report to regional managers. Regional teams undertake inspections of Local Offices (LOs) and Branch Offices assessing their compliance with prescribed internal control procedures. Typically, inspections take 2-3 days for a LO and a half day for a Branch Office. Teams use a generic inspection document. Data protection issues are currently not addressed within this document. The Department has indicated that currently an Internal Control Policy is being drafted in this respect.

ICSU issue office notices and reminders to highlight the existence of the unit and to remind staff of their obligations to vigilantly apply prescribed internal control procedures including, it is indicated, those relating to data protection.

In addition, the Regional Management Teams (RMTs) undertake inspections of the LOs to assess their compliance with prescribed internal control procedures. LOs who have a responsibility for a Branch Office(s) undertake such inspections in the Branch Office(s).

At the time of the audit the ICSU indicated that it was in the process of dealing with 5 reported breach cases.

The Branch Office manager and staff are not DSFA employees but operate on contracts (see follow-up meeting with Human Resources below). The LO manager undertakes 2-3 branch inspections per year, but these would not include a particular data protection aspect. Special Investigations Unit stated that they are working to remedy this in relation to the inspection templates that are used for such inspections.

The Transaction Information System (TIS) is a management audit system that randomly selects a % of transactions undertaken on its short-term payments system

(ISTS) for the Local Office Manager to check. Where the requisite number of checks is not being undertaken, this is flagged to ICSU to take appropriate action. This seemed to the Audit Team to provide a route for increased monitoring of compliance with data protection requirements at a local office level. The Department has pointed out, however, that in its current format TIS does have the functionality to enable the selection of random ‘enquiry or read ’accesses for checking, but is exploring other options to address this issue.

It was established during a meeting with Human Resources that branch manager positions are advertised in the local and national press with successful applicants contracted to DSFA. The contract specifies that it is a condition of appointment that the branch manager shall be responsible for ensuring that data on the Department’s computer system is accessed for official purposes only, and that s/he must familiarise him/herself with the Department’s Data and Business Information Protection Policy and ensure that all BO staff comply with these requirements. S/he is paid by the Department depending on number of staff but it is a matter for the branch manager to recruit staff. Such staff must sign a contract with the branch manager and sign the Official Secrets Act, FOI Act and Department of Finance Circular 3/89 dealing with data protection.

The Department could not provide the Team with a copy of the staff contract - it was stated that this fell outside the remit of the Department as it was a matter for the branch manager. Any person recruited in this manner has access to the ISTS (Integrated Short Term Systems) system which contains benefits related information and can set up and maintain a claim, but cannot authorise/approve a claim.

It is clear from the above that from a data protection perspective branch managers act as data processors for the Department and that it accordingly is fully responsible for any access to personal data that takes place by branch managers and the staff they employ. The Department has indicated that it is aware of this legal responsibility.

4.3. Inspection of Specific Divisions & Systems

4.3.1 Illness Benefit

This section was chosen for inspection in light of the particular sensitivity and range of personal data which is processed. There is a staff complement of between 270-280 working in the section. The Team was informed that all new staff receive data protection training as part of the general Department induction course. In addition, a one-to-one meeting is held with their respective manager (Assistant Principal) where the sensitivity of the data and the responsibilities of staff in relation to the information which they will have access to on a daily basis is outlined. The section also circulates a data protection notice on an annual basis which they require staff to sign confirming they have read and understood its contents. It was also outlined that in-branch training takes place routinely to reinforce key procedures, e.g., verification of identification of callers to the unit etc.

The Team observed the live system - ISTS - and the processing of forms specifically relating to claims for continuance of Illness Benefit. Access to specific systems are available to staff via a menu page, however not all items on the menu can be accessed by staff from Illness Benefit. Staff in the unit have what is indicated as limited look-up access to the CRS system in order to assess eligibility for illness benefit (e.g., staff need to check that a pension is not being claimed or if they see a lone parent allowance is being paid, then the claimant would only receive half the amount of illness benefit). A smaller subset of staff would have again what is indicated as limited 'update' access to CRS data in order to undertake customer maintenance work on CRS when a claim is being registered or during the lifetime of a claim such as correction of a date of birth or recording of a marriage.

It was also noted that information relating to medical conditions on ISTS is confined to choosing a specific preset category from a drop down menu.

In relation to paper files, illness benefit claim forms (MC1 & MC2) are filed initially on the office floor and retained as long as a claim is open. The Team viewed the active claims files which are filed in transparent sleeves in the open plan area. Actual medical certificates themselves are stored separately in a sealed area with restricted access. The claims are subsequently filed away in the basement file store for six years for audit purposes before being destroyed. There are no physical files designated to any one individual by name but there is an electronic record retrievable via ISTS for every person who has submitted a claim. There is card access to the basement filing area where the illness benefit files are stored in a separate locked area. An inspection of this area was undertaken. Prior to reaching the secure area, a substantial volume of claims files in crates were identified outside the entrance to the store in an area immediately adjacent to the lift. This presented a clear security risk to the data in question that was fully accepted by the Department and the issue was dealt with within two days of the audit. The Department in relation to the background to this incident has pointed out that to allow for the upgrading of the shelving in the basement area all old dockets (for the years 2000 to 2007) had to be removed from the shelving. The dockets were stored in crates which were numbered. The crates were stored as far as possible in the secured area. However due to the volume of crates, some crates were stored as a very temporary measure in the lift area. The crates were closed crates loaded on top of each other. The Department considers it would not have been possible to obtain claim papers relating to a particular individual from the crates as there were no identifiers on the crates outlining the contents. The area where the crates were temporarily stored is accessible only by DSFA staff or other authorised individuals. It is also monitored by a surveillance camera.

4.3.2 Statistics Unit

This unit was chosen as part of the audit to allow for an assessment to be made of the level and type of information provided to the statistics unit to allow it to perform its function. This was to assist in an assessment as to whether procedures are in place to provide access to personal data on a need to know basis within the Department.

As part of this process, the audit team examined the terminal of the Section HEO. An inspection of the personal data on the PC highlighted a welfare payments system extract in excel format detailing all Jobseeker and related schemes claims open on a particular date that is received by FTP to the PC. The extract consists of a spreadsheet containing extensive fields of personal information including PPSN, address and personal bank details in relation to approximately 300,000 individuals. It was established that only a small number of the fields with non-identifiable data were needed to complete the relevant statistical tasks on an ongoing basis. The Team also established that the spreadsheet could be downloaded to the individual's desktop and that the USB portal was active on the machine. The information could also be emailed in its current format.

There does not appear to be any clear reason why material containing such confidential data should be circulated in this form. Such a level of detail would be deemed excessive under the Data Protection Acts 1988 and 2003. The Department has indicated that the extract as it is sent to the Stats Unit has been limited to the non-identifiable data specified by Statistics Unit from 13 April 2008.

It was further established during the course of the audit that the extract is circulated relatively widely within the Department. It was recommended that an immediate review be undertaken of the contents of the system extract and the list of recipients to whom it is circulated.

4.3.3 ACMS Child Benefit

The ACMS Child Benefit System has migrated to the new BOM system functionality as outlined earlier. In its legacy form it is no longer actively maintained or monitored. A very small amount of users based in DSFA's Child Benefit section in Letterkenny use ACMS for the purposes of gathering data in relation to historical claims (approx 15 a day, available to 80 users). The application provides 'enquiries' only. All enquiries are logged. Access is not available via INFOSYS. When transferring data to new systems, a business decision was made to only transfer data from 2002. Therefore historical data is not available through the new system.

4.3.4 Medical Certs

The Medical Certs system is used for storing and accessing information relating to doctors who provide medical certificates to patients for use in the context of claims for various benefits.

Recorded in the Med Certs system are the doctors' details to whom the certificate issued, including panel number, name and address, the PPSN of the patient and a record that a special report has been requested / performed.

The Medical Certs database resides on a server that a large group of people have access to. In this respect the Department has pointed out that not every person with access to the server can access the database. Database access is only available to people with access to that particular file share. In the current set-up of the system, it would be possible for any individual in that group (and possibly others outside of that group – technical testing would be required to ascertain how many) to take a copy of this database to their local PC, and send via email, or print, or take on a external storage device (USB key, MP3 player etc) outside of the organisation. It is not possible for the Department to track this kind of activity.

The database is protected by a 'generic' password that is known to many people. The password mechanism in use is weak and would be straightforward to break. The

Department has indicated that the 'generic' password on the database is known to about 22 users on the system plus a number of technical support personnel. In order to make use of this 'generic' password the user must be logged on to the network via an individual password.

There is limited logging, auditing and tracking taking place of what transactions happen within the database. It was not made clear exactly what level of logging activity, if any, is provided for by the application.

An overhaul of the Medical Certs application is required in order to provide levels of security that are commensurate with the data stored in the database. The security measures currently provided are weak and do not conform to best practice standards in any category. It was noted that it is planned to move this application to the SDM platform at some time in the future. The Department has indicated that this is imminent as part of a migration of the system and that a RFT has issued.

4.3.5 ISTS (Integrated Short Term Systems)

ISTS covers 3 areas: Jobseeker, Illness (as indicated above) and Maternity and Supplementary Welfare Allowance. It was set up in 1995 and is due to be converted to SDM in 4-5 years.

The ISTS system has a comprehensive logging and auditing capability whereby all updates, changes, additions, modifications, etc,. are recorded, and subsequently archived for future retrieval if required. There is currently one significant failing of the logging and auditing mechanism: A user list with given roles is circulated on what is understood to be a monthly basis to local management, who report back on whether access is inappropriate or user no longer required. Staff can only update claims based in their own location (office). There is an exception where a LO also has a branch office assigned to it. In this situation, staff from the LO with appropriate access permissions can update a claim from the branch office. A further exception relates to certain LO staff who are authorised to register or certify Illness Benefit claims.

There are approx 3,500 DSFA staff with access to ISTS and a further 1,110 HSE staff. It is the view of the Department that all these ISTS users have a business need to access the system. There are, however, concerns on the part of the ODPC that this number seems excessive and hard to fully justify from a need to know perspective. This is exacerbated somewhat by the system weakness identified above. In response, the Department has indicated that it is satisfied that all ISTS accounts are necessary to properly conduct its business. It has stated that while it can review the numbers and level of access for all users of the system, given that ISTS is an integrated system which covers a number of the main schemes administered by the Department, it seems unlikely that any such review would lead to a major decrease in the number of users who need access to the system. The Department has also requested the HSE to conduct an audit of INFOSYS and ISTS accounts to ensure that only staff who require access to these systems are provided with it.

4.3.6 Client Identity Services (CIS)

CIS was established by DSFA in 2000. It now concentrates on several core functions: a registration unit which monitors all PPSN registration activity nationwide and a separate unit with responsibility for data quality management issues. In the mid to longer term there is a PPSN replacement project in the pipeline which may consist of an additional digit being added to the existing PPSN structure or may result in a complete overhaul of the public services number.

Fraud & Error Survey

The Department's Control Division carried out a Fraud and Error Survey on the PPSN number allocation process. A copy of the survey was supplied to the ODPC. The survey estimated that only 0.5% of PPSN registrations were fraudulent (5 cases in every 1,000) with only 1 of the fraudulent applications being identified pre-PPSN allocation. Errors (as opposed to fraud) emerged as the key issue for concern with data entry errors directly affecting data quality. Since the results of the survey were received, CIS has placed a renewed emphasis on data entry and verification, drawing up a set of guidelines for all staff inputting or verifying data and organising seminars for staff which specifically address data quality management issues.

Social Welfare Act (2007)

It was explained to the Team the above Act introduced 3 additional measures to counter PPSN fraud or misuse:

- Update of 2007 Welfare Act to make the provision of false documentation in support of an application for a PPSN an offence.

- The 2007 Act also contains provisions to allow the registration authority, i.e., DSFA to retain documents it believes to be suspicious for a period of 21 days.

- This Act also removed from An Post its status as a specified body for the use of the PPSN. The status of An Post has been amended to that of an agent with a specific function in relation to scheme related payments similar to the limited roles played by other private sector entities in relation to the use of the PPSN.

Public Services Card

The Social Welfare Act 2007 was also amended to expand the Public Service Identity (PSI) of an individual to include an individual's photo, signature and death cert (if any).

CIS are working towards the rollout of the public services card in Autumn 2008 on a phased basis. It has been agreed that the initial issue of the public service card will be related to Free Travel and will carry Integrated Ticketing functionality. Final decisions such as what PSI elements will be featured on the card and related branding issues have yet to be decided. The Department has indicated that it will keep the ODPC informed of proposals and offer the opportunity to comment.

It is the stated intention of CIS that only information needed to authenticate the services a citizen has signed up for will become part of the Public Services Card

(PSC). The PSC to be rolled out will feature 'thin-client' data with no data collected on the card which could indicate or aggregate an individual's public service activities. Relevant information required to supplement a service request will only be held at the back-end by the service provider in question e.g., Irish Rail. The ODPC sought clarification as to whether the use of the public services card would be optional to avail of public services. In this respect the Department has indicated that only information needed to authenticate the individual will be included on the chip or on the card itself. A separate chip will be included on some cards to assist an eligible individual benefit from the Free Travel Scheme through automated use of the integrated ticketing network being deployed by the Department of Transport. As regards the 'optional nature' of the PSC, it will not be a requirement that every individual should carry one for identification purposes. Rather, the PSC can act as the individual's key to public services. In summary, while the use of a PSC might generally be optional, people will not be able to avail of the Free Travel scheme without a PSC once the scheme is rolled out.

Exchange/Sharing of Information

Clarification was sought in relation to the operational reliance placed upon Section 261 (exchange of information to/from the Revenue Commissioners, another Government Department, or a public body) and Section 265 (sharing of information between specified bodies) of the Social Welfare (Consolidation) Act 2005. The requirement for clarity in this area was prompted by some concern at the extent of information sharing and exchange between other public bodies and within the Department as a whole. The focus on these provisions was also linked to the increasing reliance upon the PPSN for the provision of services by public bodies. It was clarified that CIS undertakes data matching exercises and data exchange with specified bodies in accordance with the provisions of Section 265. Data exchanges between the Control Division and a range of other bodies rely upon the provisions of Section 261. The Team queried the parameters for sharing information and in what instances such sharing was legitimate, as they seemed to be at variance in several sections (261-271). The Team in this respect were advised that clarification was being sought from the Department's Legal Adviser as regards the scope of Section 261, taking into account the provisions of Section 265. In the meantime, CIS undertakes 'data matching' exercises rather than 'data exchanges'.

Over the last year, the Office of the Data Protection Commissioner has received an ever increasing number of requests for advice on publicly-funded projects or schemes involving the gathering of the PPSN. Specific problem areas were instanced by the Team in the course of the audit. In many cases, the Office has advised that use of the PPSN for a purpose not specified in legislation or for a purpose not referred to in the PPSN Register of Users (http://www.welfare.ie/topics/ppsn/rou.html) maintained by DSFA could ultimately be deemed excessive and unwarranted under the Data Protection Acts 1988 and 2003. A particular importance is attached to the Register of Users of the PPSN as a reference source by this Office. However, it is also the case that a strong responsibility rests with the Department in relation to the use made of the PPSN by bodies not specified to use it for a particular purpose. It is an offence under the Social Welfare (Consolidation) Acts to do so and the Department has indicated its acceptance of its enforcement role in this area. It has indicated that it is responsible for the issue of the PPSN following a standard registration process. The uses to which the PPSN can be put are specified in its legislation and that of other bodies (e.g.

Finance Acts) as well as being subject to Data Protection legislation. The Department has the power to prosecute offences relating to PPSN misuse that contravene its own legislation.

The Department maintains a number of documents on its website (www.welfare.ie) that set out the use of the PPSN, a code of practice for authorised users as well as a register of material from these indicating how and why they use the number.

The Department will undertake another public awareness campaign setting out the uses, including limitations of use, of the number.

The ODPC welcomes the above.

Data Feeds/Data Matching

An examination was conducted of how data feeds from General Register Office (GRO) and Revenue OnLine are managed on a daily basis. Data feeds from GRO relate to births registered. CIS issue new-borns with a PPSN on foot of notifications received from GRO. At the time of the audit, data feeds from Reachservices (operating under the aegis of DSFA) relate to registration requests to avail of online services (principally Revenue services). Such registration requires a matching process against data held on the CRS and Revenue files to take place before an individual can become a registered user of online government services. REACH functions are now the responsibility of the Department of Finance. The Department has indicated that all connections, including the connections between DSFA and Revenue, are currently being reviewed.

Requests received through Reachservices were being processed at the time of the demonstration, with staff verifying details received by accessing the CRS and Revenue address file (from 2006) to perform a cross check for the most up to date information. Once verified, if the Revenue address was established as being the most recent address, then the address on CRS was updated to reflect this. Access is also available to the GRO database to verify dates of birth and name data. Template text is used to seek further information when data submitted cannot be matched sufficiently with records held.

The section also has responsibility for records clean up in general. A report demonstrating the volume of unviable PPSN records without vital data fields such as first name, surname, address, etc., was shown to the audit team. There are 500,000 dormant accounts (no activity for more than seven years) on the system – emigrants/non-nationals/death cases. 139,000 records have no date of birth information. CIS maintained that some of those dormant accounts could easily become active again for one reason or another and that it was extremely difficult to devise a disposal/deletion schedule with the possible exception of deaths recorded which could be archived/sent to National Archives.

Third Party Data Matching Requests

The Team was informed that all data matching requests are received centrally and forwarded to CIS. In most cases external data is sent by email attachments to Operations in the Department's IT Unit and are matched by batch programme against the CRS system. Couriers are also used for transporting external disks. The

Department has emphasised that all data matching exchanges are in compliance with secure transfer procedures.

Information matching exercises and transfers to public service bodies also take place on an ad-hoc basis. The Audit Team requested examples of recent ad-hoc requests which were reviewed. It was stated that the CIS is not in a position to determine the business efficacy or otherwise of a third party's data-matching request. In many circumstances, it examines the totality of the data involved to ascertain if matching could be restricted to certain groups, etc.

4.3.7 Control Division - Regional Director's Office

Control Division undertakes matching of data on an individual's details which have been requested from third parties citing the provisions in the Social Welfare (Consolidation) Acts as the basis. From the examination undertaken, personal data is routinely received from the Revenue Commissioners, the Irish Prison Service and the Garda National Immigration Bureau (GNIB). Data has also been sourced from all third level institutions and the Department of Agriculture & Food, in order to establish if the person is receiving payments under any of the DSFA schemes. It is considered by the Division that Section 261(2) and Section 261(3) of the Social Welfare (Consolidation) Act 2005 provide a legal basis for the transfer and matching of this data.

In relation to Revenue, data on persons who have commenced employment was stated to be received on encrypted tape. Data received from the third level sector is received via e-mail and not encrypted. All data received from third parties is held on a shared database (shared drawer) within Control Division. All staff (10) within Control Division have access to all folders. There is no retention or disposal schedule for data stored within the shared drawer and overall there is no data retention policy in relation to computer or physical files within Control Division.

USB ports are enabled on all computers within the division. Physical files – mostly pre-2005 - are held in unlocked filing cabinets. In order to enter Control Division, there are no physical security requirements. It was noted that the Division is due to move to Carrick on Shannon shortly and it was stated that such controls would be in place then.

It was noted that currently information is made available by Control Division in relation to social welfare claimants to the Gardaí in Pearse Street on foot of an oral request.

In response to the above points, the Department has pointed out that Control Division comprises Central Prosecution section and Central Control section. The total staffing for the Unit is 17.5 of which 10 work in the Central Control section. A large part of the work of Central Control section relates to data matching exercises as provided for under the provisions of the Social Welfare (Consolidation) Acts. A secure shared drawer was set up to store data relating to the matching exercises. The 10 involved staff require access to the data held in the shared area to perform their duties. The vast bulk of the data held in filing cabinets in the section relates to monthly reports which are published documents. All data received from third parties for data matching exercises is stored in the secured shared drawer data base with limited access. This data is not held in hard copy in filing cabinets. Finally, new procedures have been since put in place that require the Gardaí to put the request in writing and to state that it is for the purposes of a Garda investigation.

4.3.8 Public Office (Oisín House)

Oisín House contains a PPS Registration office where applications for PPSNs are received and identities checked on a face-to-face basis prior to further central checking against the Department's systems. The Team were given a brief demonstration on the procedures and general operation of the office. Applicants fill out the relevant application form, the information from which is used to populate the data held in relation to them by the Department. They must also supply relevant identification documents to support their application. These documents are subject to checks by counter staff and the Team were shown the anti-fraud methods available to staff, including a binder containing copies of verified identification documents from around the world. They also have a system of decoding passport strip numbers ("Passport Digit Calendar") to ensure that they are valid documents as well as having equipment to verify the authenticity of these documents.

When documents have been authenticated and data is inputted to the system, it cannot be edited further by the Office staff. Copies are taken of applicant identification documents and are retained indefinitely by the Department.

4.4 Third Party Data Feeds

There are a number of entities to whom data is sent and from whom data is received on an ongoing basis. Much of this information is of a sensitive nature. The CRS system as an example takes data from a number of external sources; Revenue, FÁS, An Post and Fáilte Ireland. The Department sends information to the Central Statistics Office (CSO).

The Department's systems have numerous external interfaces including with Revenue, Bank of Ireland, FloGas, An Post, Bord Gais, etc. Details are sent to these entities regarding relevant benefits for customers. As an example, in the case of FloGas, details of customers eligible for free bottled gas are sent to allow for delivery of the service. Bord Gais and FloGas currently participate in the Natural Gas Allowance Scheme. Bord Gais is by far the largest participant, with a customer base of approximately 26,000 DSFA allowance recipients. Files are currently exchanged in respect of awards and terminations via Intelligent Application Gateway (IAG). The volumes concerned are 100 awards and 40 terminations per week. Bord Gais are currently developing their systems to facilitate electronic nightly file transfer with the Department over a leased line. FloGas have only 150 DSFA allowance recipients. There are no bulk data file transfers with this company. FloGas are enabling their systems for encrypted file exchange (PrivateFile), meanwhile a small number of awards (1 or 2 per week) are notified by phone. Bottle Gas refill allowance is paid directly to the customer's nominated financial account /nominated post office. Customer details include name & address. In the case of An Post, the Department informs it of the name and address of customers eligible for free TV licenses. The TV License is created within the SDM system and posted to the customer. An Post is given the name and address details of those eligible for licenses in order for An Post to maintain a list of TV license holders.

Local authorities for rent allowance purposes have access via the government Virtual Private Network (VPN) which secures communications from point-to-point. Various other agencies also gain access through a VPN.

Information is usually sent by external agencies to the Department using Connect Direct which is a secure transmission facility. This allows the external agency to transfer data securely and assures delivery to a specified server. Fáilte Ireland has a requirement to send information to the Department but they do not yet have the facility. Instead, they send information by email, although it is indicated that encryption is used.

IT operations have defined three secure methods by which they will send and receive information to and from third parities. At the time of the audit there was a project on-going to identify which method applies to each outside agency – and that each method is aligned to policy in this respect. That project is now complete.

Garda National Immigration Bureau (GNIB)
The Garda National Immigration Bureau was outlined to have a requirement to receive information from DSFA on a regular basis. In the case of non-EEA residents who are holders of a PPSN, details are sent to the GNIB of name and address; type of claim; Payment; where and when they sign on. The legal basis for this is specified as Section 8 of the Immigration Act 2003.

It was noted this information is sent to the GNIB on a CD, without any additional security mechanism, such as encryption etc. It was noted that a Departmental Services Officer personally delivered the CD to the GNIB and it was signed for to confirm delivery. However, this alone did not ensure the security of the information once delivered. The Department has indicated that with effect from 1 March, 2008, all bulk transfers of data with authorised external bodies are in encrypted format. It has also pointed out that its responsibilities do not extend to other agencies in their own capacity as data controllers.

4.5 Additional Findings Relating to IT Operations Group

Password resets
Given the large number of staff and the diverse locations, it is deemed impossible by DSFA to recognise all callers seeking a change of password. Help Desk staff currently utilise a very basic verification system for the caller which is clearly open to abuse. The Department has indicated that although no breaches have been uncovered, this is a recognised issue, a review of which is included in the area's business plans.

Staff and Third-Party Remote Access
There are currently multiple ways by which both DSFA staff located at home or off-site, and external maintenance contractors and suppliers, can gain access to various systems. This needs to be addressed. The Department has highlighted that there are currently three methods to access data, all of which are secure. The Department now

has a single preferred method to access data. People will be migrated to this method as resources allow.

Laptop Security
The question of security provided on laptops was acknowledged as an area of risk that needs attention where personal data is held on laptops. The Department has indicated that BIOS passwords are employed and procedures for laptop issues and losses are in place. It also highlighted that historically laptops have been used in thin client mode where corporate data does not transfer down to the laptop.

Desktop Security
There are currently two systems in place. What is termed a dumb terminal VAX system and a Windows PC system. The dumb terminal systems are secure as there is no data stored on them or access to peripheral storage. The Windows based PC's are not secured, in that users have access to all of the hard drive and CD and USB access. The Team advised that unrestricted use of USB devices is an issue that needs to be considered urgently and the Department has stated that it is currently exploring ways in which this could be progressed.

Physical & Environmental Security
A physical inspection was performed of both the ******** and ********. It was noted in both instances that a high level of security was in place at the time of the inspection, and best practice is being followed. Some minor points noted, specifically in relation to ********, were as follows:

- Picture ID is not required for ******** (although required for access to ********). Both are critical ********, and as such both should be treated uniformly.

- There does not appear to be a log kept of equipment moving in and out of the ********. The Department has pointed out that it is logged in another location.

5. FINDINGS

Good co-operation was received throughout the inspection for which the Commissioner wishes to record his appreciation.

Security of Personal Data
The audit has demonstrated that there is in place strong organisational awareness at senior management level of data protection principles. There would also appear to be a desire to follow through on this awareness at an operational level. There are challenges in this respect in an organisation as large and as diverse as DSFA. Some of these challenges were evident from the issues uncovered during the course of the audit. Instances of practice viewed revealed some inconsistencies, contradictions, gaps in knowledge, security hazards and an apparent question as to the availability of resources to actively monitor the usage by specified bodies of the PPSN. The storage of a large amount of sensitive personal data relating to illness in crates immediately adjacent to a lift area was a strong reminder of the necessity of ensuring that the risks of allowing unauthorised access to personal data are fully understood throughout the

organisation. It is accepted that a full explanation has been provided by the Department in this respect.

From an IT perspective, DSFA has a very large number of what it considers as legacy systems which do not provide appropriate functionality to be assured that access to personal data is taking place on a need to know basis only. On this issue the Department has indicated that it is currently engaged in a multi-year programme to replace the computer applications that it uses to administer its schemes and client systems. These systems are commonly referred to as ‘legacy’ systems. When these systems were originally built, it was standard practice to make them available to as many business users as possible and to audit only changes to data, whereas in the past few years it has become a requirement to limit access on a ‘need to know’ basis and to know who has read an individual’s data.

It goes on to state that the design of the Department’s new systems (known as the Business Object Model) includes better access control and facilities that allow the Department to log and query read access. The Department will replace/migrate all its remaining ‘legacy’ systems over the next 5 years or so. The speed of migration is governed by the availability of resources on both the technical and business areas of the Department (who have to continue to operate and maintain current production systems while re-engineering Departmental processes and systems) but the Department recognises the desirability, on many grounds, of completing the migration.

In view of the criticality of its main client record system, it has just completed ‘retro-fitting’ a ‘read audit’ capability.

The advice of this Office was sought in the course of the audit as to which systems should be expedited in this manner. However, this is not a matter that this Office is in a position to advise on as the Department as the business owner of the systems is best placed to make the appropriate risk assessment and devote resources appropriately. The absence of full audit trails for critical systems may prevent the Department from meeting its obligations under the Data Protection Acts in terms of processing data in a secure and safe manner. The Department has highlighted that it is not complacent or satisfied with its exposure in this area.

In this respect, it should also be pointed out that there is a need to transfer personal data to the developed systems when they are viable and to implement a policy of removing access to the legacy systems. The present practice in some cases, whatever the preferences of business users, of retaining the legacy systems on line with historical data would tend to mitigate any data protection benefits from the movement of such systems to the BOM.

The introduction of random and periodic checks of detailed access logs of members of staff over a particular period are of paramount importance. The introduction of access log checks and the practice being declared a standard check will assist the Department in deterring unauthorised access. All periodic checks should also be supported by a feedback procedure to a relevant central unit confirming such checks having taken place. As stated earlier the ICSU currently receives feeds in relation to other control procedures (Management Check System) in terms of fraudulent claims, etc., that supervisors are required to perform. The Department has undertaken to examine options in this area in relation to access from a data protection perspective.

Extent of data-sharing in the broader public service using the PPSN
Owing to the complexity of information flows within and across the Department, it was not straightforward to obtain a complete and clear picture as to the extent of data-sharing across Departments, agencies and bodies utilising data from the Department of Social & Family Affairs. It is acknowledged that there are clear procedures in place for dealing with requests for data matching exercises from Government Departments and agencies on an ongoing or ad-hoc basis. However, the level or extent of exchanges made on a 'case by case' basis across the Department, although in all probability legitimate disclosures, are not centrally recorded or logged by Departmental staff. Details of matching jobs are recorded. It is therefore difficult to estimate the volume and frequency of information sharing taking place between the Department and other Government Departments or authorised bodies or indeed other jurisdictions. An information-mapping exercise charting all personal information flows typically occurring within and between the Department of Social & Family Affairs is deemed as very worthwhile in terms of improving clarity and transparency in relation to the processing of personal data.

There is some lack of clarity in this respect as to the role performed by CIS and that of Control Division in relation to data matching. It is clear from the inspection of Control Division that a large amount of data is being sought from external agencies and bodies relying upon the provisions in the Social Welfare (Consolidation) Act 2005 for the purposes of the control of social welfare schemes. However, equally it is the view of this Office that it is unclear as to whether these provisions can be relied upon in all cases for the type of bulk data currently being sought from and supplied by third level institutions in relation to students and the Department of Agriculture & Food in relation to payments made to farmers. This is an issue of some concern to the Commissioner and it is recommended that the Department seek specific legal advice as to the full legal basis for this. Currently there is also no data retention policy in place in the Control Division. It is to be welcomed that the Department has indicated that new procedures are being developed and a retention policy will form part of those new procedures.

The PPSN – originally confined as the RSI to transactions with the Department of Social and Family Affairs and the Revenue Commissioners – is today increasingly demanded by public agencies as a condition for providing a wide range of services. Section 2 (1) (c) of the Data Protection Acts 1988 & 2003 states *inter alia* that data **"shall have been obtained only for one or more specified, explicit and legitimate purposes"**.

Legislation regulating the use of the PPSN (principally, the Social Welfare Consolidation Act 2005) provides that the PPSN can be used either by the specified bodies named in the Social Welfare Acts or by any person or body authorised by these bodies to act on their behalf. It is the Commissioner's interpretation of the Acts that equally it should only be used by such bodies for particular transactions and where the transaction relates to a public function of a public body. The Commissioner believes that in this respect the Department and the ODPC are in absolute agreement regarding the need to curb the perception of the PPSN as a potential unique identifier for a multitude of unspecified purposes by public and indeed private sector bodies. It is noted that the Register of Use of the PPSN maintained by DSFA and available from its web site does not reflect more recent, additional uses of the PPSN by specified bodies. It is recommended that frequent spot-checks be conducted on existing entries and additional information be provided as a pre-requisite for the continuing use of the PPSN for non-staff related purposes by such bodies. All entries should be updated to include and reflect all areas where the PSSN is being captured and stored.

There is room for improvement generally of data retention procedures by the Department. The Inspection Team recommends the use of a centrally devised set of retention schedule guidelines for local offices and branches based on the business needs of the users and looks forward to the publication of a set of retention schedules along with new records management policy guidelines.

6. RECOMMENDATIONS

ACCESS MANAGEMENT AND USER PROVISIONING:

- Formal Review of all access management and user provisioning based on the 'Need to Know' principle. As an example, this Office views the current user base with access to ISTS of approx 3,500 DSFA staff and a further 1,110 HSE staff as likely excessive from a business need perspective.

  Department Response: The Department's Data Access Control Policy clearly states that access to the Department's applications and associated information should be restricted to authorised individuals and for the purpose intended. The Department is engaged in a review of all aspects of data management and control and is currently considering a range of measures to enhance security arrangements so as to better ensure that authorised users are provided with the minimum functionality required to perform their roles. The Department is also engaged in discussions with external service providers in relation to access to data held by the Department – agencies have been advised that direct access provision will be replaced by alternative means where appropriate.

  The ISTS application is the system used for the registration and maintenance of most of the Department's short-term schemes and, therefore, has an extensive user base. The system is also provided to a number of external agencies to support a range of customer services and supports. In the case of the latter, access is granted on the basis of Memoranda of Agreement which clearly specify the requirement to ensure compliance with the Data Protection Acts, and that personal data will only be accessed for the purpose intended and will not be revealed to unauthorised persons. Access to the system is provided to the HSE to support payment of the Supplementary Welfare Allowance scheme which the HSE administers on behalf of the Department. The Department is currently engaged in discussions with the HSE regarding their data access requirements and they have been advised that direct access to DSFA systems will be terminated where no longer required and replaced by alternative means where appropriate.

- Where necessary, expedite the movement of what are termed by the Department legacy systems to the BOM and remove access to the legacy systems when this is done. The findings in relation to the medical certs database are deemed particularly illustrative of the need to expedite the process of moving applications to a new, more suitable platform. **Department Response:** The Department has commenced the process of replacing the Medical Certificates system as part of the current set of modernisation projects.

- Technical measures to be put in place on the basis outlined in Section 5 to facilitate identification of all user access to personal data across the Department's network. **Department Response:** The Department has incorporated this facility in its Central Records System and in the business solutions built on the new Business Object Model.

- Immediately disable generic accounts, e.g., as found in relation to INFOSYS and put a policy in place to prohibit the use of such accounts to access DSFA data. Create unique accounts only that will provide for a meaningful audit trail. **Department Response:** This is the Department's policy. All internal generic accounts on applications containing customer data have been disabled and arrangements are underway to disable all external generic accounts containing customer data.

- Procedures to be put in place for granting and removing access to systems. **Department Response:** The Department's policy is that user access privileges are authorised by the application owner and are to be revoked promptly when an individual user is no longer entitled to them. Provisioning and de-provisioning arrangements are currently under review (as referenced in response to first recommendation above).

- Agree a formalised procedure for performing password resets, under what conditions and what information is required. **Department Response:** Revised password reset procedures are currently being drafted.

- Perform an audit exercise to determine how many 'redundant' accounts exist in the OpenVMS system. **Department Response:** The Department regularly reviews dormant accounts and terminates them where appropriate. The last review took place in February 2008.

- Enhanced audit reporting functionality where reports can be commissioned and produced by auditing systems that identify trends and spikes in access.

- Review of access logs by staff at supervisor level on a periodic basis to highlight any irregular access patterns amongst staff. These reviews to become part of the set of checks that are fed back to the ICSU or other appropriate section.

- Circulation of regular ‘user trend’ reports to local unit managers for further investigation. Local Managers are best placed to identify issues particular to an area in which they work.

  Department Response: The last three recommendations above all deal with reporting on logs of user access. The Department will look at automating the examination of its access logs and reporting on anomalies uncovered.

SECURITY:

- Frequent external assessments of security (both technical and human) of the Department’s systems. **Department Response:** This is current practice within the Department and will continue. The Department has a comprehensive information risk management process which requires assessment of the technical and human aspects of information security. In late 2005 the Department engaged consultants to support an Information Risk Management project with a view to further embedding the process within the Department. The project also included an assessment of the Department’s most critical business systems.

- An immediate review should be undertaken of the contents of the system extract (ref: Statistics Unit section 4.3.2) and the list of recipients to whom it is circulated to bring it more into line. **Department Response:** This review is underway. The contents of the extract supplied to Statistics Unit have been amended to remove all unnecessary data.

- Guidance to staff in relation to the need to store personal data in a secure manner. Compliance should be monitored on an ongoing basis. **Department Response:** This is a continuous programme that has been underway for some time. Revised operational guidelines are currently being prepared.

- Review laptop security in general, and devise a strategic plan for implementing additional security measures, such as laptop encryption, in the short-term where laptops might hold personal data. **Department Response:** A review of portable computing and storage devices is currently underway. The Department is currently considering a range of measures to enhance the security of these devices.

- Ideally all disk and USB ports on all staff computers should be disabled, unless there is a clearly defined and compelling business reason that they should be accessible. Where USB keys are used, at a minimum, there should be some degree of auditing and logging of what users copy from computers to USB keys. **Department Response:** USB ports are the standard means whereby most peripheral devices are now connected to PC’s. Devices connected through these ports include keyboards, mice, printers and scanners as well as storage devices. The Department will investigate solutions for the selective disabling of devices and/or enforcing of additional security measures such as encryption. This is being addressed within the context of the review referenced above.

- Initiate a standardised approach to software development that takes security into account at the beginning of the software development life cycle. **Department Response:** The Department has a standard approach to software development, which it will review to see if additional measures need to be adopted to meet the recommendations of this report.

- All significant data protection incidents of security breach to be reported to the Office of the Data Protection Commissioner immediately. **Department Response:** The Department has agreed to report all significant data protection breaches to the Commissioner.

PPSN & PSI:

- A particular importance is attached to the Register of Users of the PPSN as a reference source. Efforts should be made to ensure it is updated by all agencies to reflect full use of PPSN and more resources should be devoted to this task. **Department Response:** The Department intends to undertake a review of the provisions of the Social Welfare Consolidation Act 2005 relating to the PPSN and will examine the feasibility of this recommendation within that context.

- Frequent spot-checks of specified bodies and their use of the PPSN based on the Register of Users should be introduced. **Department Response:** The Department will examine the feasibility of this recommendation within the context of the review referenced above.

- All specified bodies should apply to DSFA for authorisation/approval to introduce any new use of the PPSN. **Department Response:** The Department considers that the use of the PPSN by specified bodies is subject to the provisions of the Social Welfare Consolidation Act 2005 and normal Data Protection legislation. This recommendation will be considered within the context of the review referenced above.

DATA SHARING/EXCHANGE:

- Assessment that an appropriate basis exists in the Social Welfare (Consolidation) Act 2005 for the type of bulk data currently being sought for the control of schemes by the Control Unit. **Department Response:** Section 261 of the Social Welfare (Consolidation) Act 2005 provides the legislative basis for these exchanges. The provisions of the Act relating to data sharing and data exchange are currently under examination.

- There should be a focus to ensure that only an appropriate level of access to data is made available when an agency is granted access to another Department's data or vice-versa. **Department Response:** As stated above, the Department is currently engaged in a review of access provision with external service providers. Agencies have been advised that direct access provision will be replaced by alternative means where appropriate.

- At present, IT Operations have agreed 3 secure channels through which they will accept information from, and deliver information to, third parties. All third parties need to adopt these procedures to ensure the means through which it receives information from the DSFA conforms to one of the three agreed methods. DSFA needs to ensure that it will only send and receive data using one of the agreed methods. **Department Response:** The Department has implemented this recommendation in respect of data transfers to third parties and will advise them of the recommendation in respect of transfers to us. The Department will ensure that all future channels of data exchange that may be employed will also be secure.

- In terms of data transfers from third party agencies a policy should be drawn up limiting copies made and kept of such data to a minimum. **Department Response:** This will be incorporated into revised guidelines.

- Fáilte Ireland and Garda National Immigration Bureau need to immediately revise their procedures to ensure the means through which they send information to DSFA conforms to one of the three 'sure channels' offered by DSFA. **Department Response:** Fáilte Ireland already encrypts data; the GNIB will be notified of the ODPC recommendation.

- Going forward, perform an audit of the various methods by which remote access is provided, and consolidate one single avenue of access. **Department Response:** The Department has identified a preferred method of access and will concentrate on this. It also recognises, however, that other methods may be appropriate in particular circumstances as long as these are secure and auditable.

- All requests from external bodies and agencies not specifically provided for in legislation including An Garda Síochána, should be in writing and specify that the request is in relation to the investigation, detection or prevention of a crime. This would provide a more appropriate basis for DSFA to release such information in line with the provisions of the Data Protection Acts. **Department Response:** This provision is included in the revised Guidelines on Data Protection that the Department forwarded to the ODPC for observations and comment prior to circulation in the Department.

DATA PROTECTION POLICIES:

- Appropriate emphasis should be given to implementing meaningful training in data protection for the current cadre of staff within the Department in addition to the focus on new entrants. The need for this focus was clear throughout the audit. **Department Response:** The Department has been actively engaged in promoting staff information security awareness through a broad programme using a variety of media. The programme includes formal training sessions, presentations, office notices, e-learning, regular online messages, articles in Departmental magazines and posters. With regard to the formal presentations, while there had been a focus on new entrants and line management induction, these have now been expanded to include the current cadre of staff. Suggestions made by the ODPC will be considered within the context of the review of the information security awareness strategy that is currently underway.

- Section 2(1)(c) of the Data Protection Acts 1998 and 2003 provide that a data controller shall not retain personal data longer than is necessary for the purpose or purposes it was obtained. Accordingly, it is recommended that DSFA devise and implement a defined policy on retention periods for all items of personal data kept by the organisation. **Department Response:** The Department accepts this recommendation.

7. REVIEW OF PROGRESS

It has been agreed that the Department will inform the Office of the Data Protection Commissioner of progress on the issues highlighted in the recommendations and the main body of the report above, including in relation to data flows, not later than end-2008. At that time further interactions will take place in relation to any need for further dialogue with the Office on meeting data protection obligations.

8. APPENDICES

Appendix 1:	Letter of intention to audit.
Appendix 2:	External agencies that have access to 'INFOSYS'
Appendix 3:	Inspection of HRM system

Appendix 1: Letter of intention to audit.

30 October 2007

Ms. Bernadette Lacey
Secretary General
Department of Social and Family Affairs
Áras Mhic Dhiarmada
Store Street
Dublin 1.

Dear Secretary-General

I am writing to you by way of follow-up to ongoing contacts with your Department in relation to concerns about the security of personal data which it holds. I attempted to speak to you recently about the most recent reports of security breaches which surfaced in the media in mid-October. We have since received a specific allegation of a further recent breach, details of which have been transmitted to Maureen Waldron of your Department.

I am seriously concerned at the succession of reports of illegal 'leaks' of personal information – some of it quite sensitive – from within your Department. While I appreciate the constraints under which the Department operates, I know you will share my view that customers of the State are entitled to guarantees that information they give to the State system - much of it under legal compulsion - will only be used by those who need to access it and will not be disclosed to 3rd parties not entitled to receive it.

I fully acknowledge that the Department has taken certain steps to address this issue. I also acknowledge that the Department has co-operated with this Office both in relation to specific issues and the audit carried out in 2006. But I remain to be convinced that the steps taken by the Department to date are sufficient to provide the necessary level of assurance to the many individuals whose data is retained by your Department and to discharge the Department's obligations under the Data Protection Acts.

I therefore intend to undertake a focussed audit of your Department's procedures for processing personal data. This audit, to be conducted under Section 10 of the Data Protection Acts 1988 & 2003, would partly be by way of follow-up of the last, more general, audit of the Department conducted by my Office in 2006. I believe that this audit should prove of benefit to your Department in terms of offering an independent external view of the procedures in place for processing personal data and any additional measures that should be taken to guarantee the security of such data.

The audit will focus on two main clusters of issues:

(i) The measures in place to protect the security of the personal data of customers of the Department of Social and Family Affairs

- The degree of access to customer data provided to staff of the Department and to other agencies with access to DSFA databases
- Technical measures in place to identify access to personal data across the Department's network
- Consideration of what 'need to know' access entails across a large Department such as yours
- Systems in place for granting and removing access to personal data on a 'need to know' basis
- Practical measures in place to review access logs at managerial level to highlight any irregular access patterns amongst staff
- Actual steps taken to educate staff in relation to responsibilities when handling personal data
- External assessments of security (both technical and human) of the Department's systems in the past 5 years
- Known incidents of security breach over the past 5 years and details of any action taken on foot of them
- Additional security measures taken since the last audit by my Office
- Planned actions to further improve security

(ii) Establish a clearer picture of the extent of data-sharing in the broader public service using the PPSN as an identifier and utilising data from your Department.

- Appropriate level of access to data when an Agency is granted access to your Department's data and vice-versa with a particular focus on selected key Departments
- Procedures in place for dealing with requests from Government Departments and agencies and others for access to personal data held by your Department both on an ongoing and ad-hoc basis
- measures put in place for monitoring access to your Department's personal data in such instances
- Measures sought to be in place in any Agency granted such access to your Department's personal data.

I would envisage that the audit would take a number of days to complete, probably involving more than one visit to the Department. The audit team may be assisted by external security consultants. Each member of the audit team (including the consultants) will be an "authorised officer" under the terms of section 24 of the Data Protection Acts with associated rights of access to documents and corresponding obligations of confidentiality.

Given the level of seriousness which I attach to a successful audit, I have asked the Deputy Commissioner, Gary Davis, to lead the audit. I would appreciate it if you would nominate a senior member of staff to liaise with the audit team and arrange for that person to make contact with Gary Davis to arrange suitable dates for the conduct of the audit. I would wish the audit to proceed not later than January 2008.

Following the audit, a draft report, with recommendations, will be provided to your Department for comment. I would envisage the main points of the report being made public either through my Annual Report to the Oireachtas or otherwise.

In order to ensure the best possible conduct of the audit, I would be grateful if you could arrange for the provision of some background information in advance:

- A flow chart and outline description of all systems containing personal data in use currently within your Department
- A list of all external access to these systems and all Department of Social & Family Affairs access to external systems
- A list of prescribed bodies specified to gather and use the PPSN together with the legislative basis in each instance
- An outline as to the use which each prescribed body may make of the PPSN

I would be grateful to receive this material by the end of November. This is, of course, in addition to the response on specific 'leaks' to insurance companies (via Private Investigators) which I brought to your attention last June and which I expect to receive shortly.

My approach is to seek an outcome that provides a clear, realistic and verifiable path to achieving the standards expected of such a large holder of personal data. I would see this as a prerequisite to any proposals for further extension of the data held by the Department or of any further sharing of such data across the public sector.

I look forward to your personal engagement with this exercise and am available for any clarification you might require.

Yours sincerely

Billy Hawkes
Data Protection Commissioner

Appendix 2: External agencies that have access to ‘INFOSYS’

FAS
Health Service Executive
South Dublin County Council
Fingal County Council
Dun Laoghaire/Rathdown County Council
Dublin City Council
Donegal Integrated Development Team
Department of Enterprise, Trade & Employment
Department of Environment, Heritage & Local Govt. *

Central Statistics Office

* Housing Rental Accommodation Sections in the County Councils not included in the above list may have a ‘read only’ limited snapshot of INFOSYS under an agreement with the Department of Environment, Heritage & Local Government.

Appendix 3: Inspection of HRM system

This system was inspected during the course of the audit to allow for the Office to begin examining its operation from a data protection perspective. It is deployed across the civil service so any conclusions will have civil service wide applicability.

Access to the system is allocated to users within the HR Unit according to their requirements. Display-only access is available in some cases. There is a very small number of 'super-users' with administrative type access within a section of 60-70 staff overall. It is notable that the user ID of the staff member to access the system is their PPSN and it is questionable as to whether using the PPSN for this purpose is consistent with the legislative basis for its use.

Job Data/Career data do not include salary type/allowance details, *e.g.* details of salary deductions would not be known or detailed by HR. Only an individual's salary point on scale is recorded. Details of disciplinary proceedings are not detailed on HRMS. In cases where disciplinary action has taken place, a note such as "Refer to Manual File" may be inserted on the system. Only details such as infringements and flexi-clock deficits are likely to be specified. However, records in relation to absenteeism and health information are generally available to view. Reasons for sick leave are recorded on system by choosing from an extensive drop-down menu of options.

PMDS Rating information is uploaded to the system and is generally available to view by all HR staff. It would be unclear that unit wide access to this information would be consistent with the expectations of staff rated in this way. Competition results are not recorded, only information on actual promotions.