



**INVESTIGATION INTO THE SECURITY AND PROCESSING OF
PERSONAL DATA HELD IN THE DEPARTMENT OF HEALTH
AND SOCIAL SECURITY BENEFIT PAYMENT SYSTEM**

AN EXECUTIVE REPORT BY TREASURY INTERNAL AUDIT

June 2008

INVESTIGATION INTO THE SECURITY AND PROCESSING OF PERSONAL DATA HELD IN THE DEPARTMENT OF HEALTH AND SOCIAL SECURITY BENEFIT PAYMENT SYSTEM

1 BACKGROUND

- 1.1 On the 21st November 2007 it was reported in the UK national press that HM Revenue & Customs (HMRC), in the UK, had lost two computer discs containing child benefit records, which included the names, addresses and bank details of 25 million people.
- 1.2 The two computer discs were reported as being lost when they were sent through the internal mail system from HMRC offices in Newcastle to the National Audit Office in London. Whilst procedures were in place within HMRC that should have prevented such an incident happening, this incident was attributed to a breach of those procedures by an individual officer.
- 1.3 In response to this incident the Treasury Minister made a statement advising that the Isle of Man Government had high-level data protection and information security policies in place and that while there was nothing to suggest that there was any reason for concern, a review of these policies and procedures was instigated, in order to ensure compliance with best practice and to provide some assurance that the risks of any data loss had been minimised. This review was completed earlier this year. Those areas of Government where recommendations have been made were requested to provide details, to Internal Audit Division, of the planned action to be taken to address the issues raised. The issue of this report was delayed until these responses had been received.
- 1.4 A follow-up review is to take place within the next six months in order to ascertain the progress that has been made with the suggested action plans and what impact this has made with the implementation of the recommendations made.

2 INVESTIGATIONS

- 2.1 An internal audit of the security and processing of personal data held in the Department of Health and Social Security (DHSS) Benefit Payment System has been undertaken. The focus of this internal audit has been on security management (policies and organisational arrangements), information management (operational procedures and disclosures of personal data), access controls (user access and physical security) together with staff awareness and training.
- 2.2 Investigations have been conducted by staff within the Treasury, Internal Audit Division who together with a number of officers within the DHSS and other departments to whom personal information from the

DHSS Benefit Payment System is disclosed (i.e. Treasury, DOLGE, MEA and so on), have examined the procedure in place and the purpose(s) of those disclosures as part of this review.

- 2.3 Officers within Treasury, Information Systems Division have also been engaged in the review in relation to the security of information which is transferred electronically across the IOM Government network to produce benefit payments and management reports.

3 SUMMARY OF FINDINGS

Security Management

Policies & Procedures

- 3.1 IOM Government policies and procedures have been reviewed and tested to provide a degree of assurance and confirmation from the officers interviewed that they are satisfied that the staff who process information from the Benefit Payment System have an appropriate awareness of their responsibilities for information security under the established legislative framework and relevant procedures including:-

- Government Financial Regulations
- Code of Best Practice for the Maintenance of Information Security
- Information Security Policy
- Data Protection Policy
- Electronic Communications Policies
- Know Your Customer guidelines

Organisational arrangements

- 3.2 It has been confirmed that each department which processes data from the Benefits Payment System has a recognised and designated Data Protection and Information Security Officer (DPISO) who is responsible for ensuring compliance with policies, for promoting staff training, awareness and ensuring best practice in relation to data protection and information security.
- 3.3 Treasury, Information Systems Division (ISD) has been certificated to ISO27001:2005 an internationally recognised information security standard. Certification to this security standard has required that ISD implement a number of measures to protect the confidentiality, integrity and availability of information processed on the IOM Government (IoMg) network. Compliance with this security standard is reviewed on a six monthly basis through both an internal and external audit and formal accreditation of their information security management system. Such a review has recently been undertaken, which concluded that satisfactory

security measures were in place, permitting the renewal of their certification for a further three years, commencing January 2008.

3.4 The DHSS are currently finalising their work to complete a risk register which will identify business risks and the actions to be taken to mitigate the risks. **Controlling access to information**

User access controls

- 3.5 Treasury, Information Systems Division is responsible for the IoMg network infrastructure, which includes the provision of secure computer facilities for DHSS, Treasury, Police, etc. The IoMg network is protected from unauthorised access by multi-layered defences, including a Firewall, Anti-virus and Anti-spyware software etc as would be expected to safeguard the integrity of a sophisticated information technology installation.
- 3.6 The authentication and authorisation of users of network computers, computer services and systems is largely controlled via the centralised services provided by Treasury, Information Systems Division. Formal registration and de-registration procedures for granting or revoking user access to computer systems have been established and rigorously enforced.
- 3.7 The main computer suite and print services facilities managed by ISD are physically secure with the appropriate security audited externally as part of the ISD certification to ISO27001:2005. There is restricted and controlled access to the main computer room and all prints-outs and documentation that are produced for Social Security benefits are handled securely.
- 3.8 Benefit System Administrators have been clearly identified and have been authorised to produce "bulk" down-loads of data with the ability to create system reports. In addition, these staff administer the authorisation of user access to the Benefit Payments System and the use of benefit system passwords. These also provide that application groups are in place to ensure that authorised users are only provided with information appropriate to their identified roles and responsibilities and that they cannot produce unauthorised downloads of the full database.
- 3.9 Having regard to the state of technical developments and the cost of implementing information security it is considered that appropriate technical measures have been put in place to ensure the confidentiality, integrity and availability of information. These safeguards are now inbedded within the operating systems and infrastructure hierarchy.

Physical & environmental security

- 3.10 Physical access to IOM Government buildings is appropriately controlled through the use of access systems [swipe cards] and through the use of visitor books and so on. Buildings are alarmed for security purposes and the storage and handling of information within the various offices is generally adequate, although not all office environments and storage media were found to be totally satisfactory.

Information Management

Data Protection Notification

- 3.11 The Department of Health & Social Security (DHSS) has duly registered a Data Protection Notification (N000227) which includes the purpose:- "Government – Benefits Administration" as required under the legislation. The description of the purpose covers all matters relating to the administration of Social Security Benefits, including the processing of claims, payments and the provision of statistics and quality control. The Notification also confirms details of the recipients of personal information.

Data Processing Contracts

- 3.12 Data Processing Contracts (Memorandum of Agreement) have been completed between the DHSS and a number of organisations to whom they disclose benefit information. There is a requirement for DHSS to review their existing data processing contracts and to ensure that such agreements are established with all of the organisations to whom data can be disclosed.

Data transfers to the UK

Her Majesty's Revenue & Customs (HMRC)

- 3.13 Benefit information is routinely sent to the UK in accordance with a reciprocal agreement between the IOM and the UK. The benefit information transferred to the UK is more often generated on an individual basis and is paper based rather than in the form of electronic data media e.g. disc, e-mail exchange etc. The volume of data transfer is relatively low, amounting to approximately 360 General Benefit claims and around 86 Pension claims per year. The only 'bulk' transfer of information to the UK relates to National Insurance Contribution details which are submitted to HM Revenue and Customs and amount to approximately 5,000 to 9,000 records annually. These records are submitted as an e-mail attachment to a designated HMRC officer.
- 3.14 Although the DHSS Contributions Section send personal data to the UK by registered post, benefit information is generally sent by normal postal

delivery channels. Steps are to be taken to ensure that in future all personal data is sent to the UK by registered post. A formal Data Processing Contract (Memorandum of Agreement) needs to be established between DHSS and HMRC to protect the exchange of personal data.

UK System Supplier

- 3.15 A Contract is in place between DHSS and a specialist information technology company based in the UK who are responsible for the development and support of the Benefit Payment System. A confidentiality statement has been formalised with the company and is securely held by DHSS, Social Security Division, Policy Section.
- 3.16 Data has been provided to, and routinely exchanged with, the company in an electronic format on CD or DVD by ISD for system testing and support purposes. Data is normally anonymised, with the CDs sent by registered post or delivered by hand to programmers from the company when they have visited the Island.
- 3.17 However, in one recent instance personal data was found to have not been anonymised and was sent via the ordinary postal services. No valid explanation has been identified for this change in the established security arrangements and steps have been immediately taken to reinstate the former security standard. The last such exchange and dispatch of a CD containing anonymised data was sent by registered post on 3 December 2007.
- 3.18 Although data is anonymised consideration is to be given by ISD to the encryption of all future data transfers.

Data transfers within the Isle of Man

- 3.19 On Island, benefit claimant information is routinely shared with Government Departments, Statutory Boards, Local Authorities and Private Landlords. The volumes of information are, generally, fairly low and paper based, with much of the information being requested on a case by case basis, and delivered by either internal or external postal services.

Treasury

- 3.20 Electronic transfers of "bulk" information are limited to two regular submissions of benefit payment data from the DHSS to Treasury. In the first instance, this transfer takes the form of a weekly transfer of payments data between the Benefit Payments System and the Treasury Centralised Data Centre. This data transfer is handled within a secure computer network environment through system interfaces which do not

involve the use of removable media such as the Compact Discs which gave rise to the data loss in the UK.

- 3.21 The second "bulk" transfer of information involves a submission to the Income Tax Division of details of benefits paid for taxation purposes. This information is sent via the internal IOMg e-mail network, on a monthly basis and again at year end. Given the inherent risk of human error staff must be particularly aware of the risk of misdirecting email messages. Internal communication between Departments is good and regular contact amongst staff working with this sensitive data mitigates any rudimentary oversight or error.
- 3.22 In addition, a number of staff within Income Tax Division have been provided with access to view benefit information within their standard computer desk top applications. The access has been provided in accordance with The Income Tax Act 1970. However, this access may be regarded as being excessive as it not only provides officers with the information they require to process particular tax assessments, but it also provides them with the ability to view information for individuals for whom they are not processing a current tax assessment.
- 3.23 It is acknowledged that there are constraints in the design of the Benefit Payment System which may present the DHSS with difficulties in restricting system access to only those cases which require processing. The removal or restriction of such excessive access to the system may have to be considered in the wider context to ensure fair and lawful processing of personal data in accordance with the principles of the legislation.
- 3.24 A supplementary review of the processing of IOM Government Pension Declaration forms has highlighted that some improvements should be made to the administrative process of issuing the forms and to ensure the security of the confidential information returned on the forms themselves.

Offices of central government, statutory boards/authorities, etc

- 3.25 Personal data is disclosed to the Department of Local Government and the Environment, Manx Electricity Authority and Local Authorities for reasons which are consistent with the registered data protection purpose and in accordance with Schedule 9, Claims & Benefits Regulations 1987 Act which provides for the disclosure of personal data in relation to heat/lighting and rent payments. The disclosure of information is in paper format and is dispatched within IOM Government by internal mail services or externally using normal postal delivery services. No security issues were raised regarding the use of these delivery services.
- 3.26 Health Services, Family Practitioner Services have been provided with "view only" access to the benefit system in order to fulfil their

administrative role to determine the qualification criteria and to confirm that people are in receipt of benefits and are entitled to free prescriptions, ophthalmic and dental services. This access may also be regarded as being “excessive” under the act, as it not only provides officers with the information they require to process free prescription claims and so on, but it also provides the ability to view other information held in the system not relevant to the primary task.

- 3.27 As mentioned earlier, there are constraints in the design of the Benefit Payment System which may present DHSS with difficulties in restricting system access and the removal of potentially excessive access privileges to the system may have to be considered in the wider context to ensure the fair and lawful processing of personal data.

Post Office

- 3.28 The Post Office has been responsible for the handling and delivery of all internal mail across Isle of Man Government since January 2007. In addition to managing internal mail deliveries and collections the Post Office also has a separate service arrangement to open, sort and deliver all DHSS mail. At present there are no formal contracts in place with the Post Office for the opening, delivery and handling of mail and this may be regarded as not being fair and lawful processing of personal data and a breach of the Data Protection Principles.
- 3.29 It has been confirmed that the departments which are in receipt of benefit information delivered through the internal mail system have appropriate measures in place to handle and store information securely.

Human resources security

Security vetting

- 3.30 A basic level of security vetting is conducted for all Isle of Man Government staff during the staff recruitment process. All ISD support staff provided with access to live systems, regardless of the sensitivity of the data are subject to a higher level of vetting using formal police checks.

Security Awareness & Training

- 3.31 All new staff are provided with a corporate security awareness briefing. Access to IOM Government computer systems is conditional upon individuals completing the corporate briefing within 28 days. The security awareness briefing material was recently reviewed, updated and published to the IOM Government intranet for reference by staff. The staff induction process includes this requirement as mandatory.

- 3.32 Data Protection training has been provided for department Data Protection and Information Security Officers (DIPSOs) and they are key members of the organisation within their Department or Statutory Board.

Roles & Responsibilities

- 3.33 Best practice in information security recommends that specific responsibilities for data protection and information security should be clearly defined within individual job roles and responsibilities. While specific responsibilities have been included in the job descriptions issued to specific individuals within Information Systems Division steps need to be taken to clearly define responsibilities within a number of other parts of the organisation. There is a lack of consistency in personnel practice in relation to such descriptions.

4 CONCLUSIONS

- 4.1 While appropriate technical and organisational measures are being taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data it is clear from the review that improvements are required in some areas and that departments cannot become complacent about ensuring the confidentiality, integrity and availability of information.
- 4.2 In the local context it is worth acknowledging the role of the Government Information Security Officer and the proactive influence of the Data Protection Supervisor who have worked enthusiastically to improve matters and raise awareness in this area to the benefit of Government as a whole.
- 4.3 It is evident that the potential risks surrounding the access to downloading of, exchange and distribution of such sensitive data within the Isle of Man Benefit Payment System is not subject to the same exposure as that reported in the UK.
- 4.4 The procedures employed locally are generally robust, the use and exchange of such data is treated responsibly and professionally within the business purposes for which the data is recorded.
- 4.5 Whilst the review has focused upon a single application (Benefit Payments System) it is generally accepted that the framework of information security will apply across all other similar applications such as Income Tax Division, V.A.T. applications etc. Each will have its own particular hierarchy of access controls and security features to safeguard the data and ensure that it is used solely for the purpose collected.
- 4.6 Whilst there can never be a failsafe assurance given to the procedures in place, the framework of controls tested as part of this review support the

opinion that the information security provisions surrounding the Benefit Payment System are adequate.

5 RECOMMENDATIONS

5.1 The following recommendations have been made by Treasury Internal Audit to the relevant departments of IOM Government for their consideration and action:-

- that Data Processing Contracts (Memorandum of Agreement) are established in all cases where there is an exchange of personal data between organisations;
- that best practice in information security is followed and that responsibilities for data protection and information security are clearly defined in specific job roles and responsibilities;
- that registered post is used in all circumstances where personal data is sent to the UK in paper format;
- that while recognising constraints in the design of the Benefit Payment System excessive access to information should be controlled to ensure the fair and lawful processing of personal data;
- that consideration is given to sending information concerning direct payments for heat and lighting to third parties by secure electronic means, rather than internal or external mail services;
- that Information Systems Division ensure that all personal data sent electronically to external, third parties is in an encrypted format;
- that a formal contract for services and a Data Processing Contract are put in place with Isle of Man Post for the handling, delivery and opening of internal mail to ensure fair and lawful processing of information and compliance with Data Protection Principles;
- that Pay and Payments Section improve their process for the dispatch and the secure return of Pension Declaration forms;
- that Data Protection and Information Security Officers ensure that an appropriate induction process is provided to all new and temporary staff and that a programme of refresher training is provided to existing staff who have specific responsibilities for data protection and information security defined in their job roles and responsibilities;
- that where necessary suitable security arrangements are implemented to ensure the secure storage of archive records.

K C McGreal CPFA, MAPSA

Chief Internal Auditor