

**KIERAN POYNTER**

***1 Embankment Place  
London WC2N 6RH***

The Rt Hon Alistair Darling MP  
The Chancellor of the Exchequer  
HM Treasury  
1 Horse Guards Road  
London SW1A 2HQ

14 December 2007

Dear Chancellor

**Data Security at HMRC**

In accordance with the terms of reference you set for my review, I have prepared the attached short progress report focusing on two key questions. Those are 'What urgent measures should be taken?' and 'What exactly happened?'

My work is far from complete and my conclusions will develop as the work progresses. But I have seen no evidence thus far that would lead me to conclude that the statement given by you to Parliament was inaccurate.

To avoid prejudicing any possible outcomes from the ongoing enquiries being conducted by the Metropolitan Police Service and the Independent Police Complaints Commission, I will not name individuals involved in the incident, and by necessity what I can say about the facts of the matter is limited.

I am pleased to report that all the HMRC officials I have met, from Dave Hartnett the acting Chairman down, have been cooperative. He has expressed his determination to learn from these events and create the world class data security environment you would expect in HMRC.

Yours sincerely

A handwritten signature in black ink, reading 'Kieran Poynter'. The signature is written in a cursive, flowing style with a long horizontal stroke at the end.

Kieran Poynter  
Chairman and Senior Partner of PricewaterhouseCoopers LLP

# Introduction

1. My terms of reference can be summarised in three parts:
  - 1 To consider and advise you on what urgent measures should be taken to improve data security at HMRC;
  - 2 To consider the circumstances surrounding several losses of data and in particular to establish the exact chain of events which led to the loss of Child Benefit Data in October 2007;
  - 3 Having regard to the findings derived above and a broad ranging review of HMRC, to make recommendations designed to achieve the very high level of data security that you would expect at HMRC.
2. During the first three weeks of my review I have given top priority to the first part but I have also made good progress on the second part. The third part of the review has just been started. Accordingly, I will report progress below on the first two parts only.

# SECTION 1

## URGENT ACTIONS TO IMPROVE DATA SECURITY

3. I am pleased to tell you that the first actions I would have recommended had already been taken by HMRC before I began my review. These are:
- A reminder to all staff from the Chairman of HMRC of the importance of data security with some specific guidance;
  - The appointment of a senior official to the new post of Director of Data Security;
  - The appointment of Data Guardians in each area of HMRC;
  - The imposition of a complete ban on the transfer of bulk data onto removable media without adequate security protection such as encryption;
  - The disabling of the download function on all personal and laptop computers in use across HMRC to prevent their use to download data onto removable media.
  - The utilisation of secure couriers and appropriate tamper proof packaging in the transport of bulk data stored on removable media.

More recently HMRC has issued further guidance to its staff concerning the use of removable computer media.

4. I have recommended a plan to HMRC to take stock of every type of data transfer currently in use whether by electronic or documentary means, and a challenge process designed to eliminate any unnecessary transfer and to assess the security, and authorisation levels, of those which are deemed necessary. I have suggested that this analysis should be performed initially by appropriately experienced senior officials in each business unit, and will address transfers within HMRC as well as exchanges with other parties. That initial assessment would then be subject to review by the Director of Data Security and by me. This recommendation has been accepted and is currently being implemented.
5. I have recommended this approach for several reasons:
- It seems likely to be the quickest way to cover a large complex organisation like HMRC;
  - It will help to ensure that my review does cover every aspect of HMRC;
  - It will allow me to focus on analysis rather than gathering data; and perhaps most importantly;
  - It will involve a large number of HMRC officials who can play a vital subsequent role in developing a culture of improved data security across HMRC.

6. Those actions coupled with the heightened awareness of data security resulting from recent events should substantially reduce the risk of a major loss of personal data in the short term.
7. On starting this review, my immediate impression of HMRC was one of complexity, both in terms of its many constituent parts and its matrix management structure. In particular I found it difficult to relate roles and responsibilities amongst senior management to accountability. When I first mentioned this to Dave Hartnett he said that HMRC management shared these concerns and that they have also been highlighted in HMRC's Capability Review. He told me earlier this week that he was about to announce a new simpler organisation structure with a clearer accountability framework at Executive Committee level. This should make it much easier to make and implement recommendations on data security as my review progresses.
8. The longer term solution will rely on a combination of factors which I will address as the review progresses. As envisaged in my terms of reference, these include the management accountability framework, tone from the top, culture and training as well as technical measures.
9. I have agreed with HMRC to make interim recommendations as the review progresses, with a shared ambition that my final report will record that my recommendations have been fully implemented or that implementation is in progress.

## **SECTION 2**

### **What exactly happened?**

#### **Approach**

10. I am seeking to establish the facts by a combination of interviews with all those concerned and the examination of relevant documents, emails and other evidence. I have decided that a complete understanding of the events leading to the loss of data in October 2007 relies on an understanding of how the request for access to data in March 2007 was handled. Accordingly, my interviews and reviews of documents, emails and other evidence covers the period from that earlier request through to the date on which the data was lost.
11. It is important to ensure that this work does not disrupt, or prejudice, the parallel investigations being undertaken by the Metropolitan Police Service and the Independent Police Complaints Commission ("IPCC"). I have also sought to minimise the impact on the individuals involved, and the ongoing operations of HMRC, by carrying out the majority of the interviews in conjunction with the IPCC.
12. To ensure an accurate record of each interview is captured, in accordance with IPCC standard procedures, detailed manuscript notes will be taken of each interview which by necessity is time consuming. Each interviewee is offered the alternative of having their interview tape recorded, which is quicker. So far most of them have preferred not to. Interviewees will also be given an opportunity to read the notes when typed and confirm their accuracy or give corrections.
13. I have started a forensic review of the email correspondence between those HMRC officials known to have been involved in these events and that work is continuing.
14. I have also commenced a dialogue with the National Audit Office ("NAO") which is conducting its own review. I have been promised full cooperation by the Comptroller and Auditor General but I don't plan to discuss the matter in detail with his relevant staff until some further interviews with HMRC officials have been completed.

#### **Progress**

15. Good progress is being made, with about half the initial interviews completed and arrangements are in place (or shortly will be) for the other interviews I have planned. Experience suggests that some second or third interviews might be required after the first round of interviews to clarify some points of detail.
16. I am aware that an email dated 13 March 2007 has been published indicating that a senior manager in HMRC had knowledge of a request for access to Child Benefit data in March 2007, by virtue of being a copy recipient of that email. The email was sent at an early stage in the chain of events, before any final decisions about the mechanisms for delivering the data and the extent of the data to be provided had been made. That email on its own does not prove that the official actually took a decision in relation to the

manner in which HMRC should have responded to the request for data. This is just one example of the numerous copies of potentially relevant emails that I have been given but which may not in the aggregate represent the complete picture. As mentioned above, I have instituted a forensic examination of emails between officials involved during the relevant period so that I can be satisfied that I have all the evidence on which to base firm conclusions.

*This report has been prepared for and only for The Chancellor of the Exchequer and HM Treasury in accordance with the terms of reference published on 23 November 2007 and for no other purpose.  
PricewaterhouseCoopers LLP does not accept or assume any liability or duty of care for any other purpose or to any other person to whom this report is shown or into whose hands it may come.*