Report of The Independent Investigation:

breach of data security in the VFS online UK visa application facility, operated through VFS websites in India, Nigeria and Russia

L M Costelloe Baker
16 July 2007

Contents

Background

1. UKvisas is the joint Home Office and Foreign and Commonwealth Office Directorate responsible for visa processing and associated matters. VFS is a private sector commercial undertaking based in India, and part of the Kuoni travel group. UKvisas contracted with VFS to operate a visa application facility in some countries for people applying for visas to enter the United Kingdom. One part of the VFS facility was a website through which visa applicants could apply online; this online facility was run by VFS in India, Nigeria and Russia through local websites. The VFS online facility was separate from UKvisas and Home Office and Foreign and Commonwealth Office IT systems.

2. VFS and UKvisas were contacted in mid-May 2007 by an IT journalist, Mr Davey Winder, who had been told by Mr Sanjib Mitra, an Indian national, that he knew how to access details of other visa applicants on the VFS online application facility. Mr Winder passed the story to ITN and it led the Channel 4 midday and evening news on 17 May. That evening, The Lord Triesman, then Parliamentary Under Secretary of State at the Foreign & Commonwealth Office, issued a statement saying that the Foreign & Commonwealth Office would "conduct an immediate thorough and independent investigation into this reported breach". Mr Winder and Mr Mitra also put details of the apparent security breach on their personal websites.

3. Discussions between UKvisas and VFS immediately following the approach from Mr Winder concluded that the VFS website was not secure. UKvisas required VFS to close down the online visa application facility worldwide on 16 May and the site remains closed.

4. It was alleged in the news story that Mr Mitra first drew the technical problem to the attention of UKvisas, VFS and the British High Commission in India several months earlier. UKvisas and VFS have traced separate emails to them from Mr Mitra to this effect sent in December 2005. VFS took some remedial action in January 2006 but this appears to have been ineffective in solving the problem.

5. Applicants in Nigeria had reported a similar problem in April 2006, when VFS took remedial action.

Terms of Reference

6. I have been appointed by the UK Secretary of State for Foreign and Commonwealth Affairs as the Independent Investigator to investigate this apparent breach of security in the VFS online visa application facility, operated through the VFS website in India, which appears first to have been identified by Mr Sanjib Mitra in December 2005 and most recently drawn to VFS and UKvisas' attention in mid-May 2007. I attach, at Appendix A, the full Terms of Reference.

7. For the purposes of this investigation, I act in the capacity of Independent Investigator. I am also the Independent Monitor for Entry Clearance refusals with Limited Rights of Appeal, a Statutory Postholder reporting to the Foreign Secretary on the handling of visa applications in cases which do not attract a full right of appeal to an independent tribunal. Given that role, I am reasonably familiar with UKvisas' work, and that of its commercial partners, though I am robustly independent.

8. A key element of my investigation has been to ascertain the facts surrounding the apparent security breach and to report on them. I have been able to pursue relevant

lines of inquiry that were not readily apparent at the outset, but subject to this latitude, the focus of my investigation has been:

- the circumstances surrounding the apparent security breach of the VFS online visa application facility, as described above,
- issues directly associated with this apparent security breach, including the scale of the problem and its likely significance for those who used the online facility during the relevant period,
- steps taken to address the security breach,
- recommendations for further action that I consider may be necessary to address the problem and the consequences thereof.

9. The terms of reference confirmed that my investigation would cover the following specific areas:

(i) what were the personal data protection requirements when VFS were contracted to provide the application handling service;
(ii) what precautions were taken at the outset to ensure that VFS's IT system complied with data protection requirements;
(iii) what security compliance checks were undertaken as a matter of routine;
(iv) what happened when the technical loophole was first raised in December 2005, what steps were taken to rectify the problem, and the circumstances surrounding the closure of the online visa application facility following the communication by Mr Winder in May 2007;
(v) insofar as it is reasonably possible to ascertain this within the framework of this investigation, how secure has the website been and to what extent has data from the website either been stolen or misused; and
(vi) any recommendations that I consider appropriate for the future safe handling of data by VFS and/or UKvisas and as regards any remedial action that I consider ought to be taken in respect of any issue arising from the apparent security breach.

Evidence base

10. In order to prepare this report I have had:

- a folder of background information and evidence from UKvisas;
- facts and circumstances reports from UKvisas and VFS;
- written responses to my questions from UKvisas and 4 members of current and former UKvisas staff; VFS; the Border and Immigration Agency; the Security Services.
- correspondence with visa applicants Mr Mitra from India and Mr S from Nigeria; with DL a colleague of a further applicant from Nigeria; and with Mr Winder, an IT security journalist.
- discussions with the UK Government Chief Information Officer, the Foreign and Commonwealth Office Chief Information Officer, Foreign and Commonwealth Office IT security advisers, a Departmental Head of Security and Assurance; UKvisas' staff in India, The Office of the Information Commissioner, CESG staff;
- a media search;
- independent legal advice;
- an opinion from The Office of Government Commerce;
- independent IT security advice;
- an opinion from GovCertUK
- meetings with UKvisas and VFS in the UK and in India.

Facts and circumstances

11. UKvisas, established in 2002, used to handle all parts of the visa application process itself. Rapidly rising numbers of applications meant that it became difficult to manage the Public Sector Agreement targets which imposed tight turnround times, for example processing a straightforward application within 24 hours. Queues formed outside the busier Posts, opening up opportunities for exploitation by queue marshals, touts and agents. UKvisas explored ways of managing the problem and, starting in India, began to enter into a series of commercial partnerships with private sector organisations which could assist with practical administrative functions. Although the remit of the commercial partners varied from place to place it is important to emphasise that they take no part in the decision on whether the applicant should be issued with a visa. Decisions are made by UKvisas staff, known as Entry Clearance Officers; issue of a valid UK visa normally allows entry to the UK for a specific purpose and period.

12. Commercial partners, such as VFS, may provide the relevant Visa Application Form and offer visa related information, they may receive the form, application fee and supporting papers, sending those papers to UKvisas at the relevant UK diplomatic mission, known as a Post. Once UKvisas makes the decision, it can forward that to the applicant via the commercial partner. Applicants pay an administrative handling fee to UKvisas, determined under a Consular Fees Order. Until April 2007, commercial partners could charge an additional handling fee to the applicant, though as UKvisas guidance confirmed in 2003, applicants must always be able to lodge their application direct with the Post so that the additional handling fee was optional.

13. UKvisas says that the introduction of outsourcing to the UKvisas network developed on an ad hoc basis following successful pilots in Manila and Cairo during 2002. Initial outsourcing contracts signed by UKvisas were relatively short term, and a number of different country-specific contracts were signed by UKvisas and VFS during the period and in the regions covered by my investigation. Outsourcing began in India in early 2003.

14. Also in 2003 UKvisas developed an online application process called visa4UK. **It is important to note that this is a wholly separate system from the online application system developed and provided by VFS**.

15. After a pilot period in 2003, a contract was secured between the Secretary of State for Foreign and Commonwealth Affairs and Visa Facilitation Services (VFS) in relation to services in India for the period from 1st September 2004 until 31st January 2007 for outsourced application handling as outlined above. VFS would receive an application, enter the data onto its systems and transfer the data by CD to UKvisas' Posts.

16. The contract also allowed for an expansion of the services provided, UKvisas varying the manner in which applications are to be processed. The India Contract provides at clause 30.3:-

> "The Authority shall have the right to vary the Services at any time, subject to the Variation being related in nature to the Services being provided, and no such Variation will vitiate the Contract."
>
> Section 4.1 provides - "The Contractor will without the need to increase the fee charged by the contractor to visa applications, establish bandwidth connectivity so as to create a Virtual Private network between all its Application Centres, Operation

Centres and the High Commission in New Delhi and the Deputy High Commissions in Mumbai, Chennai and Kolkata for all future applications detailed below.

Those future applications included at a) Introduction of on line applications.

17. The online service in India was launched 10 August 2005. VFS developed the online IT system, which so far as the application questions were concerned, was tailor made in accordance with a specification from the British High Commission (UKvisas) in India. I attach, at Appendix B, typical questions asked of applicants for a visit visa.

18. I note that the information for website users said that "VFS shall not disclose or allow access to any personal data provided by the Foreign & Commonwealth Office or acquired by VFS during the execution of the contract other than to VFS personnel or those lawfully concerned with the execution of the contract".

19. I have been told that the main reason for not using the visa4UK online system was that it works in a closed loop for security reasons and could not be linked to the data collected by the commercial partner and sent to UKvisas. **It is important to note that the VFS online system is not connected to the secure UK Government information system used to process visa applications.**

20. In the early stages, the online application route was only available to employees of companies which UKvisas had prior approved as members of the Business Express Programme. Online applicants could apply for visas as visitors, visitors in transit (though not Direct Airside transit), or as work permit holders and their dependents.

21. The online system in India was extended later to handle applications from UKvisas' Trusted Partner Network. This included Tour Operators from March 2006 and students applying through a Trusted Partner from July 2006. From start-up to closure in May 2007, the India online site handled around 80,000 applications.

December 2005

22. On 21 December 2005, at 18:44 GMT, Mr Sanjib Mitra emailed UKvisas and VFS to warn that applicants using the online system in India could view other applicants details by changing the number on the URL[1]. He explained that doing that revealed individuals' confidential information and that was not only detrimental to the applicant but also posed a serious threat to travel and visa related impersonation and identity theft. He said that he had stumbled upon this when he incorrectly entered his wife's details.

23. Mr Mitra says that only the visa feedback section of the British High Commission replied to him with a polite e-mail, and then no follow-up took place.

24. VFS accept that they received Mr Mitra's email on 21 or 22 December 2005. They did not let UKvisas know that a problem had been reported.

25. On 3 January 2006 at 12:32 GMT a member of UKvisas London based headquarters staff notified its Information Technology Unit of Mr Mitra's email. I have been told that a brief reply was sent to Mr Mitra saying "your e-mail has been forwarded to colleagues who manage this project".

26. Soon afterwards, at 12:51 UKvisas' IT Unit emailed a colleague to explain that the website was not UKvisas' and was operated/designed/managed by VFS in India. The

[1] URL is a means of locating something by describing its network 'location'

author noted that what Mr Mitra was saying had "really serious potential impact on UKvisas as there was a site which had a wide open security flaw operating in India which has the same look and feel as UKvisas' own product, and clients will automatically think of it as UKvisas' product". The author noted the potential impact for UKvisas if identity was stolen as a result of this flaw, and despite the fact that the site design/management had nothing to do with UKvisas, the failure would be critical. He asked to discuss the situation.

27. At 16:12, a member of UKvisas' staff asked if other VFS websites had been checked.

28. At 19:34 UKvisas' IT Unit emailed a UKvisas' manager in India explaining that if the allegation was true there was a significant problem. The author explained that he had tested the allegation, noting that in accord with standard industry practice, anyone accessing the website to retrieve an application had to enter two pieces of information including their passport number. On that basis the system was not wide open to security breach as to access data someone needed two separate pieces of information one of which could be a receipt number. The concern was that Mr Mitra had included a web address with the receipt number as the final part of the web address and "if that is the back door into the system then there really is a problem". He asked UKvisas in India to take this up with VFS, saying that although the service was not managed by UKvisas, he would appreciate an answer from VFS.

29. UKvisas' manager in India passed the enquiry to VFS. On 5 January 2006 at 14:15 IST, VFS replied to say that the problem would only arise if the applicant followed the link given on the site www.ukinindia.com. The author said that "VFS had already resolved the problem and at any point in time, applicant will never be able to view the URL. Also, on all pages the right click is disabled and cannot view URL from there either".

30. On 10 January 2006, UKvisas management in India met with VFS. There is no record of this meeting but UKvisas' recollection is that the security breach was not discussed. VFS recalls that the meeting discussed further expansion of their services.

Nigeria and Russia contracts

31. The Foreign and Commonwealth Office entered into further contracts with VFS, trading as VF Worldwide Holdings, for visa application handling services in Nigeria:

    1. Contract between the Secretary of State for Foreign and Commonwealth Affairs and VF Worldwide Holdings ("VFW") in relation to services in Nigeria for the period from 1st March 2006 until 28th February 2009;

    The Contract provides at clause 38.3:-

    "The Authority shall have the right to vary the Services at any time, subject to the Variation being related in nature to the Services being provided, and no such Variation will vitiate the Contract."

    Section 4, clause 2.4 provides - "The Authority may from time to time vary the manner in which applications are to be processed. Any variation will be confirmed in writing to a representative of the Contractor."

32. The Foreign and Commonwealth Office entered into further contracts with VFS, trading as VF Worldwide Holdings, for visa application handling services in Russia:

    2. Contract between the Secretary of State for Foreign and Commonwealth

Affairs and VF Worldwide Holdings Limited ("VFW") in relation to services in Russia for the period from 7th April 2006 until 7th April 2007.

The Contract provides at clause 39.3:-

"The Authority shall have the right to vary the Services at any time, subject to the Variation being related in nature to the Services being provided, and no such Variation will vitiate the Contract."

Section 4, clause 4.1 provides – "The Contractor will at a future date agreed with the Authority, introduce further data entry services. These services will be provided without the need to increase the fee charged by the Contractor to all visa applicants, and subject to the terms of Russian Federation Law."

33. In both Nigeria and Russia the online system was available to all types of visa applicant, other than EEA family permits. There was no user ID or password necessary to access the system. In addition, the online form was an exact replica of the paper based visa application form.

34. In Nigeria, from start-up in April 2006 to closure in May 2007, the online site handled around 18,900 applications. The Russia online site handled around 1,400 applications from September 2006 to May 2007.

35. There appear to have been no reported instances of inappropriate access to personal data in the Russia online system. The manager who signed the contract confirmed that when he left in February 2006, VFS were then in discussions with a local Russian agency to find and operate the application centres which were to open later that year. There had been no thought at that time of an online visa application system. To the best of his knowledge the notification of a technical loophole first raised in India in December 2005 was not communicated to anybody in Moscow at the time. The contract that he signed had been provided by UKvisas and given that UKvisas were happy to give the contract to VFS and that the visa issuing Posts in India, under the auspices of VFS, were operating normally, Moscow had no reason to suspect or question the confidentiality of VFS' IT system.

April 2006

36. In Nigeria, on 4 April 2006, very soon after the online system went live, DL emailed VFS to complain he could see other applicants' details.

37. VFS replied on 7 April 2006 thanking DL for the details and saying that IT colleagues would set the problems right and he would revert back. VFS emailed again the next day, to say that on checking with the central server, they were not able to retrieve the application details. VFS IT personnel confirmed that dummy applications made were being generated without any problems whatsoever and all test runs were successful. VFS offered one of their IT engineers to assist in the event of any problems whilst filling out the form.

38. On 11 April 2006 at 19:25 Mr S emailed Visa Enquiries Nigeria to say that online visa applications in Nigeria were not working properly and personal information was not safe. He suggested using a password instead of passport number and surname because anyone can access an application once these details have been entered. He complained that no-one was replying to e-mail enquiries. His personal experience was that information on other applicants can find their way into other applications and he asked why, and for guarantees to allay these fears.

39. Mr S received an automated reply "*Thank you for your query. This is a very busy period for the Visa Section, and this mail box is not looked at as frequently as we would like. You may wish to visit the following sites, which should answer most queries regarding visa requirements and processes: www.ukvisas.gov.uk (general information) and www.britishcouncil.org/education/qdu/intex/htm (student specific information)"*.

40. Mr S resent his email to Consular Services Complaints.

41. The following day, DL emailed VFS again at 18:15. He had tried to re-enter details of an applicant whose data was lost previously but it was irretrievable. He had found himself in someone else's application. The 'patch' applied by VFS didn't work and he explained further problems in that the only way to move on is to move back before attempting to once again move on.

42. VFS closed the application system in Nigeria at this point.

43. On 13 April 2006 at 13:38: Public Visa Enquiries emailed Mr S "*Your message has been passed to UKvisas for reply as we are responsible for the United Kingdom's visa operation overseas. I shall pass on your concerns to my colleagues in Lagos and ask that they reply to you direct. I regret that, owing to pressure of work, it may take a little time for them to answer your message. However, under Government service delivery standards, you may expect to receive a substantive reply within a maximum of 20 working days"*.

44. Later that day, at 15:36, VFS emailed Mr S, explaining who they were: the commercial partners of the British High Commission in Nigeria. VFS noted the inconvenience that Mr S had experienced whilst applying online and offered heartfelt apologies. The author said that VFS had had a few similar complaints and were sincerely addressing the issues on hand. He explained that VFS had temporarily suspended the online application format in an attempt to redress the technical and security issues. He offered assurance that all precautions were being taken to protect the data from any misuse. VFS would resume the upgraded online format from 19th April 2006. He thanked Mr S for taking the time to write in.

45. Later that day, UKvisas manager in Nigeria emailed VFS asking them to confirm whether the online facility had been suspended and the VFS website was informing customers accordingly. He asked VFS to reply to Mr S.

46. I asked VFS in Nigeria to confirm how many complaints they had received as the email to Mr S referred to *a few*. The relevant manager recalled that although he did not have details, he could remember only the 2 complaints noted about access to personal information. Other complaints related to problems with printing the form and being unable to access the online application system. He noted that the latter problem was caused by wrong entry of the Bank receipt number and Passport Number by the applicant. These two fields were reconciliatory fields to the applicant's identity and any error would not allow the applicant to proceed.

47. From 17 to 25 April 2006, VFS's consultants, A, performed tests on the Nigeria online application site, recommending that their findings and recommendations were applied to the Russia site. A found, amongst other things, that because of *"in-proper variables handing data security was highly affected. All possible variables has to be elemenated and to be fetched from the database as and when required"* and "*there were a few pages where data was being passed from one page to another in the form of a query string. It is harmful to pass data in this fashion as it's a security laps*."

48. On 18 April 2006 VFS in India emailed UKvisas in Nigeria confirming 2 issues the second being relevant to this investigation: *Access to data of other applicants: this was the key problem caused by a coding error which, unfortunately, could not be solved by the patch that was applied. We have had the software thoroughly reviewed, and our IT team has done extensive testing that was completed last week. To be on the safe side, we have engaged an external agency to perform an independent testing –which should be over by next Tuesday (25 April). Thereafter we will enter some dummy records from Nigeria in a final phase of testing*. VFS aimed to re-launch its website by 24 April assuring UKvisas that this time they would get their act right. VFS apologised for the unfortunate lapse and were being doubly careful that there were no problems this time.

49. UK visas has confirmed that to the best of its knowledge, no further complaints were received about inappropriate access to applicant data.

February 2007

50. UKvisas standardised outsourcing arrangements in February 2007 with two commercial partners, one of which is VFS. References to contracts in this report, unless otherwise specified, relate to the earlier contracts with VFS for India, Nigeria and Russia.

May 2007

51. On 11 May 2007 some time before noon IST, Mr Mitra used the public notification section of MI5's website[2] drawing attention to the weakness in the online system in India, noting his concerns that it had not been resolved, despite his earlier warning. He thought there was a terrorist threat if identities could be stolen. Mr Mitra was able to trace that an address that looked as though it was MI5 had looked at his personal blog on just before 13:00 IST on 11 May, he having published the blog the previous day.

52. On 13 May 2007 Mr Mitra began an email exchange with IT journalist Mr Winder, drawing attention to a blog in which he had set out his concerns that the weakness in the online system in India had not been resolved. He had traced who had looked at his blog and believed that MI5 London had accessed it on 11 May. He was concerned that he had not had a reply, nor had anything been done about the problem. He explained that he could provide information on how to access the weakness but he was not posting this on his journal for obvious reasons. Mr Mitra then explained how to access the online system weakness providing a random URL to use for a test.

53. Mr Winder was, on 14 May 2007, able to change numeric identifiers within the address and access the visa application data of six different applicants stretching back over an 18 month period. The data revealed was extensive, including passport numbers and expiry dates, family data, business data, travel details. He took screenshots of the data to provide evidence of the breach and I had seen copies of that evidence.

54. Mr Winder emailed The British High Commission in Dhaka, Bangladesh on 14 May 2007 at 13:26 UK time to inform that he was about to publish a story exposing what he described as the huge hole in the VFS UK website. He asked for official comment on how this could still exist after it had been reported to both VFS and the British High Commission a year ago. He asked about the steps being taken to deal with this and prevent personal data being exposed in this way.

55. Later that day at 14:37 IST VFS emailed Mr Winder confirming that they had asked

[2] The UK Security Service

their IT team to conduct an investigation. Mr Winder offered to provide further information. VFS said they would keep the offer in mind.

56. Also later that day, at 16:39 Mr Winder emailed UKvisas enquiries to let them know that he had uncovered a serious security threat which allowed anyone to see full visa application details including personal data and passport numbers. He confirmed that he had reported it to VFS who promised an immediate investigation. He asked UKvisas what they proposed to do about such a serious security breach which could be used for ID theft. He explained that the security breach had been reported to VFS and the British High Commission a year ago and the site remained open. It had been reported to MI5 a couple of days ago – but still remained open. He had proof from an informant and had seen this in action. He was about to publish this story.

57. VFS emailed Mr Winder twice on 15 May 2007, first to ask for further information and then to confirm that the problem seemed to be resolved. Mr Winder was glad to hear the problem had finally been dealt with and had checked for himself confirming that he was now unable to see applicant data using the URL modification hack.

58. Also on 15 May 2007 The British High Commission in Dhaka contacted UKvisas' management in Bangladesh asking if action was necessary on Mr Winder's email. UKvisas' manager contacted VFS saying that the email needed to be taken seriously asking them to investigate and comment. VFS replied to confirm that were aware of the problem and had taken action.

59. Also on 15 May 2007 Mr Winder contacted VFS, asking them to confirm that the problem had been solved globally. VFS confirmed that it had been.

60. Also on 15 May 2007, VFS emailed UKvisas in India to confirm that they had asked their consultants, T, to look into the issue. They explained that the breach of security was not possible on Internet Explorer browsers but there was a possibility that it could be viewed on an Opera browser or some tailor made browser. T had fixed that and data leakage was not possible any more. T had assured VFS that the solution was fool proof and any applicant would not be able to see any other applicants' details. VFS explained how the data leakage had occurred: "*When application form is generated it is created as a reference number.html file. Reference numbers always created in a series. Hence if you have a URL which is possible to be viewed on an Opera browser or some tailor made browser, you can connect, change the reference number and view applicants forms. This was noticed yesterday (14 May). Multiple tools available and being generated on a daily basis*". The solution imposed was "*Started using session which gets created per browser and is accordingly stored in the server. Each and every browser will have a separate session number and we will use the number to generate the html file. Solution has been implemented and tried to view other applicants data and unable to do so in any of the browsers"*.

61. Also on 15 May 2007 Mr Winder contacted Channel 4 News with details of his story.

62. UKvisas says that on the afternoon of 15 May 15 May 2007, UKvisas in India contacted by telephone a member of the UKvisas' Commercial Partners' Programme in London.

63. UKvisas in India also emailed Mr Winder to explain what had been done to resolve the problem. They asked for details of the person who had drawn attention to the problem as UKvisas had no record of receiving an earlier notification, and certainly would have acted on it if it had been received. UKvisas wanted to re-assure the applicant that it took personal security and customer service very seriously. Mr Winder replied with the

details and explained that the problem was not restricted to Opera browsers – anyone could access full visa application data by changing the numerical identifiers on the URL.

64. UKvisas headquarters says that on the afternoon of 15 May 2007, UKvisas in India phoned a member of the UKvisas' Commercial Partners' Programme in London. They note that when the threat of imminent media cover became apparent, the matter was referred to a Director on 16 May.

65. UKvisas headquarters says that on 16 May 20007 they phoned VFS in India who asserted the website was now secure. UKvisas says it decided that the safest course of action was to ask VFS to close down the online application facilities in India, Nigeria, and Russia until such time as a proper assessment of their security could be undertaken.

66. On the same day, UKvisas in India emailed VFS to pass on Mr Winder's comments. They asked if VFS had had an allegation from Sanjib Mitra a year ago that there were insecurities in the system.

67. On the same day, UKvisas in India contacted Mr Mitra for information. Mr Mitra was happy to cooperate and agreed that what had happened needed to be understood so that this type of security breach can be prevented in the future. A UKvisas manager then had a telephone discussion with him.

68. Also on 16 May 2007, VFS emailed UKvisas in India to say that the consultants, T, were still to provide full data on the investigation.

69. Also on 16 May 2007, VFS confirmed that the website link had been removed for online applications in India, Nigeria and Russia, on UKvisas' direction.

70. VFS then had a series of emails with Mr Winder about the technical reasons for the breach. Mr Winder assumed that VFS was keeping application data within an unsecured database, access to which was possible by anyone with the correct URL to identify a particular record as applied to them. He noted that this kind of security by obscurity only works if the URL remains obscure and it was too easy for someone to stumble on the right URL by accident, and once they have access to the basic URL structure they then have access to the entire database. VFS asked if they could use Mr Winder's services for the betterment of its business. Mr Winder confirmed that other obligations prevented that.

71. The breach of data security by the VFS online site in India featured on Channel 4 news on 17 May 2007.

72. The contract with VFS for India expired on 31 January 2007. On 17 May 2007, it was in the process of being extended. UKvisas was expecting the agreement to be signed during the following week.

73. On 21 May 2007 at 15:42 UKvisas Public Enquiries section emailed a colleague to say "*grateful if you could deal with this enquiry* (Mr Winder's e-mail of 14 May*). Not been opened until today because we are short-staffed. I have not acknowledged. You will note that The Enquirer intends to publish*".

74. On 22 May 2007, UKvisas headquarters notified all entry clearance issuing Posts of the facts, so far as they were known at that date. It had set up a data integrity project team to co-ordinate the follow up action necessary to mitigate the reputational and business risks.

75. On 23 May 2007, UKvisas' project team noted that VFS had not properly taken down its Nigeria site, UKvisas' staff having found that they could gain access. The team noted that the fault had not been found on the India or Russia sites.

What were the personal data protection requirements when VFS were contracted to provide the application handling service?

76. In terms of the Data Protection Act 1998, [DPA] "data" is information that is processed automatically (for example, as part of a computer database) or which forms part of a relevant filing system (which is, in essence, a paper based filing system that is structured so that the data is easily accessed in a similar way to a database held electronically). "Personal data" is data which is biographical of a living individual and from which data (or from which data and other information in the possession of the data controller) that living individual can be identified. The information collected by UKvisas as part of the visa application process is biographical of living individuals in that it contains names, addresses, dates of birth, etc of applicants for visas. That data is held by UKvisas electronically so the information is personal data for the purposes of the DPA. UKvisas accepts that position.

77. Sensitive personal data is defined in Section 2 of the DPA as any personal data consisting of information as to:

    (a) the racial or ethnic origin of the data subject,
    (b) his political opinions,
    (c) his religious beliefs or other beliefs of a similar nature,
    (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
    (e) his physical or mental health or condition,
    (f) his sexual life,
    (g) the commission or alleged commission by him of any offence, or
    (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

    UKvisas' Visa Application Form requires applicants to provide information on their place of birth, which may be construed as information on racial or ethnic origin, and on criminal convictions, so it collects sensitive personal data. A visa applicant who has a civil partnership with a UK citizen may also be providing information about his or her sexual life.

78. The DPA regulates the processing of personal data. The term "processing" is to be understood broadly and covers almost anything that someone could conceivably wish to do in relation to data. It covers obtaining, recording or holding data or carrying out any operation or set of operations on the data, including –

    a) the organisation, adaptation or alteration of the data;
    b) retrieval, consultation or use of data;
    c) disclosure of the data by transmission, dissemination or otherwise making available; or
    d) alignment, combination, blocking, erasure or destruction of the data.

79. The **Data controller** is the person who (either alone or jointly or in common with other persons) determines the purposes from which and the manner in which any personal data are, or are to be, processed. The contracts noted above are silent on who is the data controller, though UKvisas accepts that it is a data controller in terms of the DPA.

80. I note that UKvisas is not separately registered as a data controller with the Information Commissioner, but relies on the Foreign & Commonwealth Office's registration.

81. The **Data processor** is defined as the person (other than an employee of the data controller) who processes data on behalf of the data controller. The contracts noted above do not stipulate who is the data processor as such; however, it is probable that in terms of the contracts the Supplier, VFS, would be considered the data processor in terms of the DPA.

82. The principal obligations under the DPA upon a data controller which are relevant to this matter are:

    1. For the data controller not to process personal data except in accordance with a valid notification made to the Information Commissioner which sets out the sorts of data processed and the purposes for which it is processed; and

    2. For the data controller to comply with the eight data protection principles.

83. VFS, as a data processor, is not required to register with the UK Information Commissioner.

The Data Protection Principles

84. The Principles are**:**

    1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

        a) at least one of the conditions in Schedule 2 is met, and
        b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

    2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

    3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

    4. Personal data shall be accurate and, where necessary, kept up to date.

    5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

    6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

    7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

    8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

85. It appears as though UKvisas is required to comply with all eight of the data protection principles in its processing of personal data and if it engages a data processor to process personal data on its behalf, UKvisas is responsible for ensuring that the data processor complies with the principles. The first, seventh and eighth data protection principles are of particular relevance.

86. **First Data Protection Principle** requires that:

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

If the personal data includes sensitive personal data, UKvisas must meet at least one of the conditions in each of Schedules 2 and 3 of the DPA.

In Schedule 2, UKvisas meets condition 5(a), namely that the processing is necessary for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

Condition 7(1) (c) of Schedule 3 is in similar terms and is similarly met.

More generally, when considering whether information has been processed fairly, regard is to be had to the method by which the information is obtained, including, in particular whether any person from whom the information is obtained is deceived or misled as to the purposes for which it is processed.

Where, as in this case, data is obtained from the data subject, the data controller must ensure so far as practicable that the following information is supplied or made available to the data subject:

a) the identity of the data controller;

b) the purposes for which the data is intended to be processed;

c) any further information which, in the circumstances, would be necessary to enable the processing of the personal data to be fair.

87. I note that the version of the visa application form in use in 2005 had a Data Protection Act statement *The Foreign & Commonwealth Office is processing the personal data on this form and related data for the purposes of promoting and protecting the interests of the United Kingdom and its citizens abroad. The data may be disclosed to other UK Government Departments and public authorities.*

88. I note that in 2005, some applicants in India were concerned about use of the personal data supplied by them and raised complaints. An investigation by VFS into a "Probable Data Leak" in June 2005 concluded that complaints relating to data use had arisen because VFS allowed "temporary staff" to collect information from applicants in its waiting areas and that this information was used/sold for marketing purposes. VFS assured UKvisas that only those people who had voluntarily completed a questionnaire would have their details passed on.

89. I note that the Functions Requirements and Guidelines document dated October 2002, as an Annex to the commercial partnering tendering exercise says, at Clause 8, that the Partner may secure additional sources of revenue through advertising subject to the agreement of the British High Commission. I am concerned that until the complaints, UKvisas seemed to be unaware of the collection of data from applicants in the waiting areas. It is easy to see how applicants could confuse the information being asked for by VFS in a waiting area with the information required by UKvisas in the visa application form. UKvisas noted that it should reconsider its policy of allowing VFS to gather information, and possibly its policy of allowing advertising in visa application centres.

90. **Seventh Data Protection Principle** requires that:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Anyone who accesses personal data is processing that personal data and accordingly, unauthorised access to personal data is unauthorised processing.

UKvisas are obliged in terms of the seventh data protection principle to ensure that no unauthorised access to the personal data occurs. They must take appropriate technical and organisational measures to protect the information.

In deciding what measures are appropriate regard is to be had to:

a) the nature of the personal data;
b) the harm that might result from its misuse;
c) the technology available to the data controller;
d) the costs likely to be incurred in putting in place an appropriate level of security.

Measures must be taken both at the time of the design of the processing system and at the time of the processing itself to ensure security is maintained. Legal guidance issued by the Information Commissioner offers some examples of security risks that should be addressed and suggests, for further advice, reference be had to BS 7799 and ISO/IEC Standard 17799.

Where a data processor is engaged, the data controller must ensure that the data processor is capable of maintaining adequate security and actually does so.

A written contract must be put in place with the data processor that:

a) ensures that the data processor only uses and discloses personal data in line with the instructions of the data controller; and
b) requires the data processor to take appropriate security measures.

91. I note that the contracts that were relevant for India, Nigeria and Russia in 2005 and 2006 do not contain comprehensive provisions, but do contain some relevant provisions.

92. **Eighth Data Protection Principle** requires that:

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The countries of the European Economic Area are the member states of the European Union together with Iceland, Liechtenstein and Norway. The countries or territories currently considered by the European Commission to have an adequate level of protection for personal data are Argentina, Canada, Guernsey, the Isle of Man and Switzerland. In relation to the USA, the European Commission considers that an adequate level of protection is offered where a company signs up to the "Safe Harbour" scheme.

Where the European Commission has not expressly decided that a country has an adequate level of protection, a data controller may still transfer personal data to that country if it is satisfied that the circumstances of the transfer provide for an adequate level of protection for that personal data.

Paragraph 13 of Part II of Schedule 1 to the DPA provides that:

An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to—
(a) the nature of the personal data,
(b) the country or territory of origin of the information contained in the data,
(c) the country or territory of final destination of that information,
(d) the purposes for which and period during which the data are intended to be processed,
(e) the law in force in the country or territory in question,
(f) the international obligations of that country or territory,
(g) any relevant codes of conduct or other rules which are enforceable in that country or
territory (whether generally or by arrangement in particular cases), and
(h) any security measures taken in respect of the data in that country or territory.

Where the data controller can comply with one of the exceptions set out in Schedule 4 to the DPA, it is not required to comply with the eighth data protection principle. Of those exceptions available, only two are thought to be relevant to this matter. Firstly, the data subject may have given their express consent to the transfer of the personal data. Secondly, a transfer may be exempt if the European Commission approved "model clauses" are used in the contractual documentation governing the transfer. The Model Clauses that govern this matter would be those approved in Commission Decision 2002/16/EC dated 27 December 2001 in which the European Commission approved model clauses for transfers from data controllers in the EEA to data processors outside of the EEA.

93. In outsourcing the handling of applications to commercial partners outwith the European Economic Area, it appears that UKvisas was not transferring data for processing in the generally accepted sense, but rather collecting data that had been obtained by the partner from an applicant. If UKvisas' decision is conveyed to the applicant through a commercial partner, it is expected to be in a sealed package so that the partner acts as no more than a courier.

The relevant contracts

94. The contract with VFS relating to India in 2005 did, at clause 17, provide that VFS should "take all measures necessary to comply with the provisions of any enactment relating to security which would apply to the Authority if it were performing the services itself." UKvisas' technical requirements had been set out on a Specification Document in July 2005. This included security specifications, such as the service should be in accord

with Foreign & Commonwealth Office standards; Secure Socket Layer (SSL) should be used to provide confidentiality, integrity and end point authentication; data is to be deleted 15 days after collection. It would, in my view, have been helpful to include more specific guidance on the requirements of the Data Protection Act because UKvisas retained responsibility overall

95. I also note that the India contract does not deal with the more specific issue of access to VFS's records by UKvisas as the data controller, in order to ensure compliance.

96. The contracts with VFS for Russia and Nigeria, signed in 2005 and 2006, contain identical data protection provisions. These go further than the contract relating to India and include requirements to ensure "all appropriate technical and organisational measures are in place in order to protect the Authority's personal data as may be required by the DPA and shall not transfer personal data outside the European Economic Area without the Authority's express written consent." I note that neither of these two contracts discusses in any further detail what such measures would be nor does it grant access rights to the "Authority" to ensure such measures are in place.

Extending the services provided

97. Whilst the terms of the contracts noted above afforded the opportunity to amend how the services were to be provided, the amendments proposed and subsequently put in place were fundamental and, in my view, should have instigated a review of the contractual arrangements in place at the time to ensure that processes were in place from a data protection perspective. Data Controllers have an on-going responsibility to ensure compliance with the DPA, given the fundamental change to the operation of the Services this should have led to a formal review, at the very least from a data protection perspective.

What precautions were taken at the outset to ensure that VFS's IT system complied with data protection requirements;

98. There is an understandable tension between those who run the day to day business and who want to get on with things, and those whose role is to ensure the safety and security of IT systems and personal data. There is evidence of that tension in much of the background information provided to me in the course of my investigation. During 2004 and 2005, exchanges between UKvisas' Posts (not only in India) and headquarters and IT staff, though mostly business like were, on occasion, tetchy. The service providers in Posts wanted haste and to hand over more administrative burden to the outsourcers. Outsourcing companies, including but not limited to VFS, were understandably keen to help in order to grow their businesses. IT and data professionals urged caution, and often needed to explain why simple solutions could not work.

99. UKvisas has no record of asking the Foreign & Commonwealth Office IT security advisors [ITSAs] for advice in relation to the contracts with VFS, and the move to an online application system. The ITSAs have no record of being asked for advice. I conclude, therefore, that such advice was neither sought nor given.

100. The ITSAs main role is to provide security guidance, policy and advice to Foreign & Commonwealth Office IT projects in accordance with official guidelines. They carry out investigations into IT security breaches and incidents, carry out reviews and provide general advice. I note my concern that the Department of 5 staff was, apparently, short of one adviser for nearly a year as that may impact on its ability to provide timely assistance and that can add to the tensions noted above.

101. I note, also, that the former organisation, the National Infrastructure Security Co-ordination Centre, an interdepartmental organisation responsible for giving Information Security advice to and devising best practice for government and certain elements of the private sector, considers that if it had been asked for advice, its view would have been that the project did not qualify.

102. VFS considers that UKvisas tested the online system before it went live and provided email correspondence to support its view. My interpretation of that correspondence, from August 2005, is that UKvisas was testing basic functionality, mirroring what would be the applicant's experience.

103. UKvisas' view is that VFS conducted some functional testing on the IT fabric to test that a certain level of functionality had been achieved in order to facilitate the required business process. UKvisas' current view is that little or no effectual security testing took place. That appears to be correct and I note that VFS did not appear to have had a formal security function, and thus an effective security procedure to cover software development and testing.

104. VFS and UKvisas agree that no third party penetration tests were carried out in the development phase of the online system or after it was launched. This is a serious and very basic failing.

105. The online service was set up with password user authentication and Verisign encryption. UKvisas say that there is no evidence that the user authentication and Verisign encryption were properly implemented. VeriSign provides trust services, including authentication, validation, and payment needed by Web sites which are conducting trusted and secure electronic commerce and communications on the Internet. VeriSign authenticates organisations, enabling users to verify a site and communicate

via Secure Socket Layer (SSL) encryption. This protects confidential information, such as online forms, from interception and hacking.

106. Although it is agreed that VFS did have Verisign accreditation in place the expert view is that the certificate verification policy was such that it rendered the security measure ineffective because certificates are distributed on line and authentication is not robust.

107. My IT security advisers have also noted that SSL encryption is a commonly misunderstood area of web security, noting a misconception that using a certificate provided by a Certificate Authority, such as VeriSign provides an enhanced security environment.

108. UKvisas recently obtained an expert assessment of the basic data security provided by the VFS online website. The findings were that the site had many security weaknesses, and that many of these weaknesses were amongst the most understood and documented security concerns in the computing industry. The expert view was that none should be present within a securely designed website.

109. I note that during the technical investigations, several screenshots provided by VFS highlighted wider security concerns. These screenshots of the management console used to access and configure the firewalls also showed users actively engaged in Skype[3] conversations and logged onto webmail[4] packages. These entities are considered to have poor security when used in isolation. Using them whilst accessing security device management consoles shows that standard acceptable usage policies are either not in place or not followed.

110. In relation to the online system for Nigeria, I note that some testing did take place in December 2005, though it appears to be limited.

111. There were some basic security measures. VFS stored details of online applications in its database for 30 days from the date of the application after which the details should have been purged. This 30 day period allowed an applicant to retrieve and complete an application if, for example, they needed to break off to find the answer to a particular question. Details were purged once VFS received the printout of the application form. VFS confirmed to me that if an applicant did not proceed, the personal data was purged automatically after 30 days.

112. I note that in a business planning document of 15 July 2005, UKvisas anticipated that the online applications would be held on VFS's servers for 15 days, and would be deleted automatically thereafter.

113. The fundamental security weakness was that a routinely created temporary file continued to remain on VFS's server after the automatic deletion process. Thus Mr Winder, who took screen shots of the application details he was able to see in May 2007, accessed applications that had been made in February 2007, well before the 30 day or 15 day purge period.

114. In addition to these technical assessments, I formed my own view that VFS procedures in relation to passwords for its own data users fell far short of even basic good practice. That view has been confirmed by a recent (June 2007) gap analysis report for VFS in relation to its work in specific visa application centre. VFS staff did not each have a

[3] Skype is an Internet Protocol (IP) based voice and message transfer system that runs on a PC

[4] webmail is a generic name for electronic mail (e-mail) viewed by using a web browser instead of a mail package such as Microsoft Outlook

unique user ID and password and there was inadequate advice provided on password confidentiality. Although this issue is not directly related to unauthorised external access to personal data provided to and processed by VFS, I mention it as it demonstrates a very poor level of real understanding of information assurance and data security. There has been, in my view, inadequate protection of data security within VFS itself.

Office of Government Commerce

115. As evidence of the lack of data security awareness by VFS emerged in the course of this investigation, I became concerned that UKvisas may not have secured adequate assurance of VFS's ability to operate appropriate data security measures when the contracts were first entered into, nor when the services were expanded into online. I asked The Office of Government Commerce [OGC] to conduct a procurement review and report to me accordingly. I will be providing a copy of that report to UKvisas.

116. I have also obtained and examined many of the relevant documents and the OGC report supports my view that UKvisas did not follow best procurement practices in acquiring some of the visa support services.

117. OGC recognised that the context for the earlier contracts was the urgent business pressures to reduce visa applicant queues but noted that;

- some contracts appear to have been let with and then used in an area where supplier capability has not been fully investigated;
- service levels with a corresponding service credit regime to encourage continuous high performance do not appear to have been defined in the earlier – India – contract;
- there does not seem to be have been consistent and effective project and contract management for the earlier procurements and contract lifecycles.

What security compliance checks were undertaken as a matter of routine;

118. I have found, with the assistance of expert advice from two sources, that ongoing data security protections were missing or wholly inadequate. VFS says that all of its IT applications underwent unit testing and integrity testing but there was no formal third-party penetration testing done for online applications. UKvisas notes that it did not carry out its own security compliance checks. There is no evidence that security testing was discharged periodically through life of the service, as known exploits and threats changed.

119. VFS indicated that its webservers and database servers are hosted at an independent internet centre, S and as part of security management, S conducted a vulnerability assessment for VFS providing a monthly report. I asked VFS for the reports from December 2005, January 2006 and April 2006. VFS then confirmed that it subscribed to the advanced managed security service in July 2006, so the reports I had asked for could not be provided.

120. A later report from the hosting company, S, has been examined by IT experts, who consider that the details within the report do not provide all of the information required for a standard vulnerability report, and appear to merely list the state of patching of the server infrastructure. They noted that the report highlighted the existence of a Windows 2003 server that had Service Pack 2 installed, recommending that this equipment should use the earlier Service Pack 1. This was, in the expert's view, a fundamental mistake that, if implemented, might have resulted in regressing the security of the product because, for example, any new patches or security enhancements delivered through Service Pack 2 would be lost.

121. My independent IT advisers have provided a helpful and technically detailed report, which I shall, in due course, provide to VFS and UKvisas for their information. From the information available, they noted that authorisation on the website was ineffective for a number of reasons. The application had not, for example, been designed to require authorisation for Mr Mitra to view the information that he accessed accidentally. The application appeared to create, and then allow public access to certain files in publicly viewable directories on the webserver.

122. My IT advisers also noted that the tester who owed a duty of care to UKvisas was able to view a user's security question from the database using an SQL injection technique. Structured Query Language (SQL) is a platform independent way of interrogating databases and SQL injection is a well known (in the industry) method that can be used by an attacker to bypass the intended security controls of a website if these security controls are poorly configured.

123. I note also that VFS were not collecting SQL logs. As part of the normal operation of an SQL database, logs are generated which reflect activity of that database - these are typically configurable, and can include a record of write, modify, deletion of data. The lack of SQL logs means that the probability of being able to detect SQL injection was low. IT experts noted that the log collecting mechanism was of low integrity as logs were left to reside on servers for significant periods of time without specific protection.

What happened when the technical loophole was first raised in December 2005, what steps were taken to rectify the problem, and the circumstances surrounding the closure of the online visa application facility following the communication by Mr Winder in May 2007;

December 2005

124. The answer to the first question is simple: very little, and what was done was inadequate. VFS took what it thought was adequate technical action . UKvisas accepted VFS's word and did not pursue the matter further.

125. What should have happened, as best practice, is that an immediate investigation would have tried to identify the scope and detail of the problem in terms of how many times the breach had occurred and who had exploited it. From that it would be possible to identify the number of persons who had taken advantage of the vulnerability and the extent of exploitation. The investigation should have gathered and secured evidence, and confirmed its findings in a formal written report.

126. VFS has said that it did not report the problem to the British Deputy High Commission (UKvisas). UKvisas appears to have notified VFS in January 2006. In my view, VFS should have been obliged to notify UKvisas on a formal basis of any complaints relating to data security.

127. VFS referred the matter to its IT department, which discussed it internally and the team arrived at a solution. The solution that was provided was only tested on the Internet Explorer browser. VFS missed the point that the same solution was not tested on other browsers such as Opera, or Netscape etc. The possibility of the blocks applied not working in other browsers was not tested. VFS has confirmed that this was due to an oversight. VFS and UKvisas agree that the action taken made unauthorised access more difficult but did not prevent it.

128. I note that, from the evidence available to me, VFS would have been hampered in conducting a fully adequate investigation because it did not have controls in the hosting environment that would allow persons who had had access to the log files to be traced. In addition, if there is an absence of formal policies and procedures, an investigation cannot test findings against what should have happened and is less likely to be sharply focused.

129. There has to be a degree of mutual confidence between an organisation and an outsourcing partner. I do think that the relationship between VFS and UKvisas was perhaps too trusting and comfortable. In my view UKvisas should have ensured that it conducted its own testing to satisfy itself that any loophole had been adequately closed. VFS, UKvisas, and preferably both, should have secured robust third party penetration testing even if that had not taken place when the online system was first launched.

130. I note that Mr Mitra had only an acknowledgment, rather than a fuller reply to confirm what had been done. I find that to be discourteous.

131. I am also concerned that UKvisas in India did not notify its headquarters staff so that precautionary tests could be undertaken, if necessary, on other applications. UKvisas IT headquarters staff did not themselves follow up the referral they had made to India. The data security breach in India was not, apparently, known to other UKvisas' staff who were about to sign contracts for an expansion of the online system in Nigeria and Russia.

May 2007

132. Mr Mitra found the same data access vulnerability in May 2007. I find it reasonable that he did not contact VFS or UKvisas on this occasion given the lack of adequate response and action to his earlier notification.

133. I have been told that the Security Services followed routine handling procedures on receipt of Mr Mitra's notification. In examining the speed of UKvisas' response, I note that this did not include a notification to UKvisas.

134. I find it regrettable that it took media cover through Mr Winder before UKvisas and VFS started to take adequate action to assess if there was a problem, and the steps were necessary to resolve it. The flurry of activity after 14 May 2007 should have happened almost 18 months earlier and a complaint from an applicant (customer) should be sufficient to ensure a prompt response, active investigation and appropriate response.

135. I am concerned that neither Mr Mitra nor Mr S in Nigeria had prompt responses to their emailed complaints and that is also true of Mr Mitra's notification in May 2007. Any email might be a warning of a significant security threat and as the facts and circumstances show, there were a number of occasions when UKvisas staff were too busy to open the mail promptly even though they may have met a 20 working days target.

Insofar as it is reasonably possible to ascertain this within the framework of this investigation, how secure has the website been and to what extent has data from the website either been stolen or misused;

136. The evidence now available confirms that the VFS online application websites have not been adequately secure from start-up until May 2007, when they were closed down. There is no evidence to date that data has been misused other than the unauthorised access noted in this report.

Border and Immigration Agency

137. The Border and Immigration Agency says that to its knowledge no abuse has been identified.

UKvisas

138. UKvisas says that it has conducted extensive testing and there is no evidence to confirm that data has been stolen or misused other than a limited amount by accident and by Mr Winder the investigative journalist.

139. In this report, which is to be made fully public without amendment, it would be inappropriate, on security grounds, to detail all of the checks made by UKvisas. I can, however, confirm that I consider those checks to have been adequately thorough.

140. In order for personal data to be misused to support a visa application, the user would have to obtain a passport in the initial applicant's name and provide all of the required supporting documents in that name and those fraudulent documents would need to be sufficiently convincing to one of UKvisas' Entry Clearance Officers. Work undertaken by UKvisas has included examining the photographs of applicants who have applied for a further visa to ensure that they look like they are one and the same person. UKvisas has not found any instances that have caused concern.

141. In addition to these application related checks, there has been significant technical effort put in to check the records of the online application site. I have been independently advised that the IT based work to identify all unauthorised data access attempts appears to be thorough.

Government experts

142. On Friday 18 May 2007, GovCertUk noted press reports of a security breach in respect of a Visa application web site in India. GovCertUK receives details of computer security incidents reported by UK government departments and provides practical assistance in resolving problems.

143. On 23 May 2007, there was a routine meeting at which representatives from the Foreign & Commonwealth Office IT security staff and CESG were present. CESG is part of GCHQ [Government Communications Headquarters] which constitutes the UK's National Technical Authority for Information Assurance, responsible for providing "advice and assistance about cryptography and other matters relating to the protection of information and other material". In this context, Information Assurance refers to confidence in the processes of information risk management, aimed at ensuring appropriate levels of availability, integrity and confidentiality of information and information systems. The work of CESG is driven by the National Information Assurance Strategy produced by the Cabinet Office on behalf of the Official Committee

on Security. Within this framework, CESG provides technical Information Assurance risk management guidance, standards of good practice, advice and assurance services across government. GovCertUK is CESG's computer security incident response team.

144. At the meeting, the Foreign & Commonwealth Office discussed the issue I am investigating and CESG offered assistance which was accepted.

145. From the evidence provided to me, I am satisfied that CESG was adequately briefed and that both UKvisas and VFS have submitted material to assist CESG in its assessment. CESG provided penetration testers to try to access the online sites on 1 June 2007 and was generally satisfied that the Foreign & Commonwealth Office (UKvisas) was taking appropriate steps.

146. CESG has spent much time analysing log files provided by VFS. CESG initially focused on the logs for India and the attempts to access numerous pages by a specific IP address. This IP address attempted to access different variants of the same URL hundreds of times. Initial assessment of this was that it was automated activity. However, the size of the organisation using the IP address - a member of UKvisas business express scheme - made it equally likely that the IP address related to a computer acting as a proxy for many others within the same organization. CESG found that the lack of logs made it impossible to come to any definitive conclusion.

147. GovCertUK was asked to verify the analysis by VFS's consultant, M, of logs from Nigeria and Russia. Its assessment was that M took reasonable steps but that, again, the lack of logs meant that no meaningful conclusions could be reached.

148. GovCertUK observed that the audit capabilities of the VFS system were far from adequate for the following reasons:

i. Very few relevant logs are collected for audit.
ii. The logs collected and made available for audit cover too small a period of time.
iii. The logs are stored on the same server as the applications.

Its view is that "effective investigations into security incidents rely upon good log collection and maintenance. The inadequacy of the logs in this case has meant that CESG investigators are unable to form a detailed picture of the events that surround the unauthorised accesses reported by Mr Mitra and Channel 4 news. Keeping logs on the same server as applications means that, should an attacker penetrate the hosting system via the application, they are likely to be able to change the logging information to cover their tracks, thus making any meaningful investigation impossible".

Media cover

149. UKvisas did consider whether it was obliged to notify all visa applicants that there may have been a breach of personal data security. In the absence of such notification, I have looked carefully at the degree of media cover which might have alerted anyone who was concerned.

150. The story of the apparent breach of the online visa application services provided by VFS in India was covered in several Indian newspapers and websites. On 18 and 19 May it featured in the Economic Times/India Times. It also featured on 19 May in the Hindustan Times, Decca Herald (Bangalore) The Telegraph (Calcutta) and The Tribune (Chandiarh). And on 20 May it was reported in The Times of India. The gist of the reporting was that

"Britain has suspended its online visa application facility from India after the personal data of thousands of Indians was compromised due to flaws with the online system. There is a looming suspicion that personal data may have been stolen. The Government have ordered a probe into the security lapse.

470,000 Indians each year apply for a visa to visit the UK with some 50,000 applying on line. UK Shadow Immigration Minister, Damien Green called it an "Indian Visa Fiasco". "Another IT shambles from the government with serious implications for security. A potential treasure trove for terrorists and identity thieves".

The British Information Commissioner, the government's data privacy watchdog, has demanded a 'full explanation' from the Foreign Office. The applicant (Sanjib Mitra) noticed the lapse in April last year and alerted VFS and the British High Commission. Mr Mitra e-mailed the company but got no reply. He also e-mailed the British High Commission and received a reply 2 months later to say they would look into it.

Visa processing in India has been contracted out to a private Indian company, VFS Global. Following the revelation online services were suspended in India as well as Nigeria and Russia where VFS provides online visa processing facilities.

In February, the Foreign Office awarded VFS a 5 year contract worth £190m for visa processing.

The Foreign Office said that the VFS system is only used to record the details of applicants applying on line through VFS and to allow applicants to see how long it will take to get their passports back. It is not connected to the secure UK Government information used to process the applications".

151. I note that none of the correspondence generated and published on websites referred to a specific, rather than general, concern about misuse of data.

152. In addition to the television news reporting in the UK, specialist IT journals and websites covered the issue, including PC Pro, The Inquirer, PC Plus and Tech.co.uk, Computer World UK, Computer, Digital Lifestyles, The Register, Gurgaonscoop (an Indian IT online magazine).These publications may have been seen by IT workers who have applied or who were intending to apply for a UK visa. I also note that Mr Mitra's and Mr Winder's blogs may have been accessed by people with an interest though they will not have had wide circulation.

Applicants

153. In June 2007, UKvisas staff in India conducted a limited survey by adding questions to a routine customer satisfaction form. Whilst 21% of the 185 respondents knew that the online application system had been suspended, only 14% knew why. There was no testing to confirm whether the understanding was accurate.

154. UKvisas has contacted members of the Business Express Programme in India to see if members of their staff had reported concerns. UKvisas has not had any adverse responses.

Complaints

155. I note that in Mumbai in particular, and in India generally, UKvisas says that it did keep complaint logs and that complaints relating to VFS were expected to be referred to a

UKvisas' manager. I note, however, that the initial reaction to the May 2007 notification was that UKvisas in India could not trace Mr Mitra's December 2005 complaint. I do not consider that UKvisas has adequate, or adequately robust data to confirm that there have been no further complaints. I do note, however, that UKvisas did take action on the 2 complaints made in Nigeria and that I have had no evidence to confirm that there have been any complaints other than the 3 known of.

156. Given the open door that has been present on the online application site since inception I have thought carefully about why there has been so little apparent misuse, other than the accidental exposure of personal data to 2 applicants and a further person assisting an applicant. These three accidental events appear to have a common factor in that they related to re-visiting a saved application. Most applicants using the online system will proceed with an application in one go and not need to save and retrieve it. This assumption is more likely to be true in India where the online system was initially limited to people who had been prior selected as trusted, such as employees of businesses included in a Business Express Scheme, or trusted tour and student agents.

157. Had CESG not been able to undertake even a limited analysis of the computer logs, then I would have assumed that many more applicants had accidentally walked though the open door, but not gone to the time and trouble to make a complaint or notify UKvisas or VFS. The logs, even with their limitations, suggest that there has been less unauthorised access than first feared. I am quite clear that is more a matter of luck than good management, sound IT skills, or adequate oversight.

Recommendations that I consider appropriate for the future safe handling of data by VFS and/or UKvisas and as regards any remedial action that I consider ought to be taken in respect of any issue arising from the apparent security breach.

The VFS online system

158. I note the expert view that the VFS online system is so poor that it should be completely re-written - one expert described it as an upside down pyramid, where piling more levels of changes and processes on the top only makes it more likely to fall over. **I recommend** that the VFS online application system should not be re-opened, though I note UKvisas' has already reached that decision. I also note that VFS has accepted that it is not an IT company and that it needs to outsource its software writing.

Visa4UK online system

159. This online system was developed by FCO Services, the main supplier of IT services to UKvisas. I note that UKvisas intends to use this system from now on and has confirmed that the Foreign & Commonwealth Office IT Security Accreditor has been asked to review the security of this programme. UKvisas has agreed an action plan with the ITSA. I note, however, the ITSA's concern that when the programme was reviewed in 2005, it was found that recommendations made in 2003 had not been implemented. Advice is just that, and there may be business needs that over-ride advice. If that is the case, the reasons for declining to implement advice must be robust and adequately recorded.

160. UKvisas commissioned a further independent check in May 2007 and whilst no major issues were identified, the recommendations that were made have, I am told, been implemented by FCO Services.

Continuing to check for unauthorised data access and misuse

161. **I recommend** that, so far as is possible with the limited material available, UKvisas should continue to ask CESG to assist in analysing the logs for evidence of unauthorised access. I have been impressed by the quality of CESG's work and eagerness to help.

162. **I recommend** that UKvisas should continue its series of checks to try to ascertain if there has been unauthorised use of personal data. It should remain alert to complaints of data misuse or unauthorised data access from applicants and ensure that any that are received are recorded and co-ordinated from a global perspective.

Current outsourcing contracts

163. UKvisas has recently - February 2007 - entered into global contracts with 2 outsourcing companies, one of which is VFS. VFS has been anxious to demonstrate to me the steps that it has been taking since May 2007 in relation to data security. I am, at the end of the investigation, now more satisfied that VFS understands the scale of the failures and what it needs to do to improve and maintain adequate performance. VFS has adopted a security testing programme, for which it should be commended, but there is still work to be done on proper procedures for incident handling. I have emphasised that it needs to be constantly vigilant, but it is UKvisas that has to be convinced that the considerable efforts currently being made by VFS are adequate, and will continue with the energy and commitment currently shown.

164. **I recommend** that UKvisas reviews the terms of the current contracts to make sure that they are adequate in terms of data protection. It should also satisfy itself that the measures now being taken by VFS are sufficiently robust. I note as one area for discussion that VFS's consultants define vulnerability according to likelihood rather than impact; this incident shows the significant impact of a very small number of incidents.

Outsourced IT programmes

165. I note that in April 2006, the Information Commissioner issued helpful good practice notes on outsourcing, attached at Appendix C. I commend them.

166. CESG has recently provided sensible guidelines and I commend them as general good practice.

1. All future outsourced projects concerning UK Government reputation and integrity should have an appointed in-house oversight executive together with independently sourced security accreditors.

2. All future IT projects should be exposed to at least basic penetration testing or webpage source code security audit. This should occur both during development and after installation.

3. In order to provide a good insight into the overall security of a product any security testing must also include the IT infrastructure and supporting packages such as databases, certification authorities, etc.

4. All code patching regimes should be included as part of the continuing site management procedure. These regimes must be included as part of the website design and appropriate policies should be established.

5. The use of 3rd party products to improve security must be considered during design and form part of the overall security plan.

167. In this regard, I note that the bigger the business, the more organisations and individuals who have to have access to personal data. In a small visa issuing Post, only an Entry Clearance Assistant, Officer and Manager will have access to an applicant's personal data, before it is checked against UK held databases. Once outsourcing happens, there are the outsourcer's staff plus its consultants and expert advisers. Despite these additional layers, UKvisas as the data controller remains accountable overall for the protections necessary. Outsourcing may relieve practical burdens from Posts, but headquarters functions and abilities need to be expanded accordingly in order to handle the increased levels of risk and risk management.

Complaints

168. I note that in general, VFS's response to complaints was courteous and reasonably prompt.

169. I note that the target turnaround time for emails sent to UKvisas' general address was 20 working days, in common with most Government Departments. This meant that neither Mr Mitra nor Mr S in Nigeria had prompt responses to their emailed complaints to UKvisas. UKvisas had not issued directions on handling email correspondence, such as skimming to check for urgent matters and instructions on escalation. UKvisas is already working on improving its handling of complaints and has recently issued guidance on recording and recognising urgency. **I recommend** that its work in this regard should

continue, accompanied by a real understanding that feedback generally helps a business to improve.

170. **I recommend** that UKvisas should write to Mr Mitra to thank him for drawing the matter to its attention. Both Mr Mitra and Mr Winder should be asked to delete permanently any unauthorised data records that they hold on their IT systems.

Governance

171. I am not satisfied that UKvisas exercised adequate governance over the outsourcing process so far as the security of personal data was concerned. IT staff in its headquarters urged caution on a number of occasions but there appears to have been no over-arching responsibility to co-ordinate those concerns and take firm action. Tensions between UKvisas' staff at Posts and internal or Foreign & Commonwealth Office IT advice were not well managed. I note that UKvisas work in India was admired as the entrepreneurial leader, developing new and imaginative ways of responding to rising demand. Organisations need entrepreneurs, but they also need clear and far sighted caution as counterbalance.

172. Governance of information assurance needs to be held at Board level, and **I recommend** that UKvisas Board includes a member with that specific responsibility.

173. I note that in April 2007, the Foreign & Commonwealth Office established the new position of Chief Information Officer. The remit is at Appendix D. The CIO's understanding is that he does not have direct responsibility for the Foreign & Commonwealth Office's Consular teams or UKvisas, which have their own IT delivery capability. He was told that UKvisas was set out on its own to meet its need to move forward quickly in terms of meeting its business roll-out objectives. He could see no reason for it needing to be outside of the main FCO IT Directorate as UKvisas' contracts would be authorised and signed up to by the Secretary of State for Foreign and Commonwealth Affairs as part of the standard financial approval process. I can understand that point of view. I liked in particular the CIO's view that IT consultancy can be bought in, but governance has to belong to the business.

174. **I recommend** that the Foreign & Commonwealth Office's CIO's understanding of the operational scope of his remit is revisited. UKvisas' role is different from the Foreign & Commonwealth Office's main duties, being a service focused, outward looking, fast changing business. It may well be that placing governance at Board level in UKvisas will provide adequate oversight, but there should be an informed decision on best practice.

175. The Government's Chief Information Officer provided me with outsourcing governance notes and I commend them;

- Good governance is build upon a great understanding and immense clarity on what it is that is being outsourced, who is accountable for what, what does success look like, knowing what to do when things go wrong and finally a culture of "one team".

- You cannot put governance around a problem you have outsourced. So to establish good governance in an outsourced world you must have mapped the state of the current processes and have mapped the processes when the outsource provider takes over. This mapping must identify what is expected to be different and the consequences of this change on the people, the processes and the technology.

- Outsourcing is a long term relationship and the contracts and governance design must recognise that objectives will change and the culture of the organisations may change. Having contracts that can flex effectively to cater for this is critical.

- Outsourcing is not abdication of the department's responsibilities and neither can it pass all of the risk to the outsourced partner. Internally within the department accountability should be clear on who has to make the outsourced operations a success, who has to deliver the clearly defined benefits and who is accountable for ensuring problems are anticipated and mitigated before they occur. The positioning of the internal accountability is key. For an outsourced operation that is key to the business it should be a Board level accountability.

- Good governance demands a "one team" "one culture" approach. Full transparency of service performance to all; full transparency of accounting to all; full membership of all meetings to all.

Summary and conclusions

176. UKvisas entered into contracts with commercial partners in order to improve the quality of experience by visa applicants in the face of rapidly rising numbers; secure adherence to the PSA turnround targets and allow Entry Clearance Officers to focus on decision making. There was, in my view, inadequate central control of the moves to outsourcing, though that has since been corrected. In entering into global contracts earlier this year, UKvisas recognised that the partnership programme had developed in a piecemeal way. The new contracts have improved consistency and are more detailed in their scope.

177. Sound security needs to be woven into the business and cannot be simply bolted on as an extra. If it is part of the fabric, it becomes the responsibility of all rather than a technical issue that belongs with an IT expert. The earlier contracts paid insufficient attention to the requirements of the Data Protection Act and to basic IT security. UKvisas was undoubtedly relieved to have the practical administrative assistance provided by outsourcing, but it did not obtain adequate third party or expert assurances that the VFS IT system was robust, even before VFS was allowed to start up an online system.

178. VFS was keen to grow a new business and to be the leader in the market. In trying to do that, it paid insufficient attention to the level of its own IT skills and abilities. I have no doubts that VFS has worked hard and successfully to provide a civilised, customer focused, visa application experience. It did, however, underestimate what was necessary in order to protect personal data to the levels expected by the UK's Data Protection Act. It would have been helpful if UKvisas had made those expectations clearer and the contracts lacked specificity.

179. UKvisas reacted inadequately to notifications from 3 people that there was a data security weakness. I do not find it acceptable for a complaint to be simply passed on to a third party - VFS in this case - for a response. If UKvisas felt responsible for replying to the complaints, it may have paid more attention to the outcomes. Whilst VFS did take responsibility for handling complaints, it did not have the technical skills necessary to resolve the issues raised.

180. In my view, there is no evidence to support any finding relating to the competence or performance of specific UKvisas' staff - the problems were far wider than that. The circumstances that led to the breach of data security from the outset, the lack of independent oversight and the failure to react adequately to Mr Mitra's December 2005 notification, were organisational failures by both UKvisas and VFS.

181. During the period of partnership both UKvisas and VFS were relatively young organisations, growing in experience and maturity. I am satisfied that, since May 2007, they have taken this problem seriously and applied significant resources to identifying weaknesses and putting into place improved skills and oversight. This has been a painful experience for them, and one which will change the nature of the partnership relationship.

L M Costelloe Baker MBA

The Independent Investigator (VFS)
PO Box 61731
London
SW1A 2WY

Appendix A: Terms of reference

Letter of Appointment and Terms of Reference

1. On behalf of the Foreign Secretary, I write formally to invite you to accept appointment as the Independent Investigator to investigate an apparent breach of security in the VFS online visa application facility, operated through the VFS website in India, which appears first to have been identified by Mr Sanjib Mitra in December 2005 and most recently drawn to VFS and UKvisas' attention in mid-May 2007. This Letter of Appointment and Terms of Reference follows discussions in recent days between you and the Legal Adviser at the Foreign and Commonwealth Office about the scope of the investigation and the support that you will require to undertake this task. I understand that you have seen this letter in draft and agree with its terms. I would be grateful, nonetheless, if you would respond formally to this letter to signal that agreement.

2. I understand that you will be in a position to commence work on this matter on 5 June 2007. Other points relevant to the timing of the investigation are addressed in paragraphs 13 and 14 below.

Background

3. VFS is a private sector commercial undertaking with which UKvisas has contracted to operate a visa application facility for those applying for visas to enter the United Kingdom. UKvisas is the joint Home Office and FCO Directorate which is responsible for visa processing and associated matters. An element of the VFS facility is a website through which visa applicants can apply online. This online facility is run by VFS in several countries through local websites. The online facility is entirely separate from UKvisas and Home Office and FCO IT systems. A copy of the applicable commercial contracts between UKvisas and VFS, as well as other preliminary documentation relevant to your investigation, will be provided to you at the start of your work.

4. VFS and UKvisas were contacted in mid-May 2007 by an IT journalist, Mr Davey Winder, who had been told by Mr Sanjib Mitra, an Indian national, that he knew how to access details of other visa applicants on the VFS online application facility. Mr Winder passed the story to ITN and it led the Channel 4 midday and evening news on 17 May. That evening, Lord Triesman issued a statement saying that the FCO would "conduct an immediate thorough and independent investigation into this reported breach". Mr Winder and Mr Mitra also put details of the apparent security breach on their personal websites.

5. Discussions between UKvisas and VFS immediately following the approach from Mr Winder concluded that the VFS website was not secure. UKvisas therefore required VFS to close down the online visa application facility worldwide on 16 May. The site remains closed.

6. It was alleged in the news story that Mr Mitra first drew the technical problem to the attention of UKvisas, VFS and the British High Commission in India several months earlier. UKvisas and VFS have now both traced separate emails to them from Mr Mitra to this effect sent in December 2005. VFS took some remedial action in January 2006 but this appears to have been ineffective in solving the problem.

7. Since 16 May 2007, VFS and UKvisas, have been undertaking an urgent investigation into the matter.

Your capacity in undertaking this investigation

8. Your position as the *Independent Monitor for Entry Clearance refusals without the right of appeal* ("Independent Monitor"), pursuant to section 23 of the Immigration and Asylum Act 1999, as amended by paragraph 27 of Schedule 7 of the Nationality, Immigration & Asylum Act 2002, gives you special expertise and insight into the visa application process. You also have an established profile as an independent monitor in this area with responsibility to report semi-annually to the Foreign Secretary. Your responsibilities in this role have necessarily given rise to issues of data protection and related questions concerning access to personal information. In your position as the Independent Monitor, you have security clearance to allow you access to security classified government information. These aspects are relevant to your appointment to undertake the present investigation.

9. We have nonetheless considered whether it would be appropriate to ask you to undertake this investigation in your capacity as the Independent Monitor. Given the terms of your responsibilities under the Immigration and Asylum Act 1999 (as amended), we have concluded that it would be appropriate to ask you to undertake this investigation as an independent expert, drawing on your expertise as the Independent Monitor, but not acting in that capacity. On behalf of the Foreign Secretary, and in view of the terms of your appointment as the Independent Monitor, I therefore affirm that, in your capacity as the Independent Monitor, you are authorised to undertake the present investigation in a separate capacity as the Independent Investigator, and to report as such to the Foreign Secretary.

Terms of Reference of the Investigation

10. The FCO considers that the circumstances of this apparent security breach must be independently investigated, and quickly and transparently reported upon. An essential element of the online visa application facility is that it must attract public confidence, including by those who use it, and it must be secure. The purpose of your investigation is therefore to investigate the circumstances of the apparent security breach, and issues directly associated with it, and to report on them, with appropriate recommendations for action. You will report to the Foreign Secretary, who will publish your report and lay it before Parliament without amendment. The FCO will also take appropriate steps to ensure that others who should see the report and may have an interest in it, including the Information Commissioner, will be provided with a copy of the report or have ready access to it. Following publication of the report, the Foreign Secretary may comment on it as appropriate.

11. A key element of your investigation will be to ascertain the facts surrounding the apparent security breach and to report thereon. In the circumstances, some flexibility in the Terms of Reference of the investigation will be necessary to allow you to pursue relevant lines of inquiry that are not at present readily apparent. Subject to this latitude, however, and in view of the imperative to report expeditiously, the focus of your investigation should be (a) the circumstances surrounding the apparent security breach of the VFS online visa application facility, as described above, (b) issues directly associated with this apparent security breach, including the scale of the problem and its likely significance for those who used the online facility during the relevant period, (c) steps taken to address the security breach, and (d) recommendations for further action that you consider may be necessary to address the problem and the consequences thereof.

12. Within this framework, your investigation should cover the following specific areas:

(i) what were the personal data protection requirements when VFS were contracted to provide the application handling service;

(ii) what precautions were taken at the outset to ensure that VFS's IT system complied with data protection requirements;

(iii) what security compliance checks were undertaken as a matter of routine;

(iv) what happened when the technical loophole was first raised in December 2005, what steps were taken to rectify the problem, and the circumstances surrounding the closure of the online visa application facility following the communication by Mr Winder in May 2007;

(v) insofar as it is reasonably possible for you to ascertain this within the framework of this investigation, how secure has the website been and to what extent has data from the website either been stolen or misused; and

(vi) any recommendations that you consider appropriate for the future safe handling of data by VFS and/or UKvisas and as regards any remedial action that you consider ought to be taken in respect of any issue arising from the apparent security breach.

13. To allow the Foreign Secretary latitude to publish your report and lay it before Parliament before Parliament rises for the summer recess on 26 July, you should transmit your report to the Foreign Secretary on or around 13 July 2007, and in any event no later than 20 July 2007. In the event that it becomes apparent that, for any reason, you will not be able to report within this period, you should raise this with the FCO, through the Legal Adviser, at the earliest opportunity to allow the matter to be properly addressed. Any delay in reporting could have wider implications, including for visa application handling and for your availability to act in your role as the Independent Monitor. In such circumstances, the Foreign Secretary may direct you to complete your report within a specified period and include in that report recommendations for the further inquiry into any aspect of the investigation that you consider should be pursued further.

14. To enable the FCO to form a preliminary view of the scale of the problem and associated issues concerning the scope of the investigation, you are asked to produce a brief status report on or around 15 June 2007, and in any event no later than 22 June 2007, setting out an initial statement of facts, the scale of the problem, and any associated issues concerning the scope of the investigation. The expectation is that this status report would not be published in its own right, its purpose being to enable a preliminary view to be taken of the scale of the problem, the resourcing of your investigation, and whether the 13 July 2007 reporting date is reasonable in the circumstances. This does not, however, preclude the possibility of the publication of this status report in whole or in part if this seems appropriate.

Associated Issues

15. To facilitate your investigation, VFS, UKvisas, and as appropriate the FCO more widely, will provide you with whatever access to information you require, as well as such other assistance and support as you may request and would be reasonable in the circumstances. At VFS, your principal point of contact should be Mr Raminder Singh Taneja, AVP Special Projects, VFS Global Services. He will act as the focal point of contact within VFS for your wider enquiries. At UKvisas, your principal point of contact should be Glyn Williams, Director, Business Development, who will similarly by the focal point for your wider enquiries of this Directorate. Within the FCO more widely, your principal points

of contact should be the FCO Legal Adviser, Daniel Bethlehem QC, and Alison Little, the Deputy Private Secretary to the Permanent Under-Secretary.

16. In due course, if it is established that the scale of the apparent security breach, and its potential consequences, are significant, it may be necessary for the FCO to undertake wider inquiries into this matter, or request others to do so, to enable those who consider themselves to have been specially affected to make representations. Given the immediate imperative of a focused, efficient and expedited investigation, your investigation should seek to establish the scale of the problem and its potential and likely consequences, as described in the preceding paragraphs. For this purpose, if your initial enquiries suggest that this is necessary, it may be appropriate for you to seek information in a targeted manner from a sample of users of the visa online application system. If you consider that wider inquiries, beyond this, of users of the online facility are necessary, this should be the subject of a recommendation in your report.

17. For purposes of your investigation, you should conduct thorough inquiries of VFS, UKvisas and others engaged on these issues as appropriate. You may also wish to contact Mr Mitra and Mr Winder. Without prejudice to your independence or the content of your report, as you gather evidence and begin to draw conclusions, it will be appropriate for you to test that evidence with those concerned.

18. In the course of your investigation, it is likely that you will have to consider confidential information, including as may be covered by principles of data protection and commercial confidence. It is also conceivable that you may have to consider security classified government information. Such information should not be set out or otherwise disclosed in your report.

19. To assist in ensuring that such information is not inadvertently disclosed, and to ensure that interested parties have an opportunity to draw to your attention factual or other points which may require clarification, you are asked to submit your report in draft to the FCO Legal Adviser four clear days before you will be submitting your report to the Foreign Secretary. The Legal Adviser will ensure that only those persons who have a direct interest in the matter will see the report in draft, and only for purposes of drawing to your attention factual and other elements the inclusion of which in the final version of the report may, for well founded reasons, raise points of concern of which you should be aware.

20. Your report may touch on issues that could be addressed in subsequent legal, contractual or disciplinary proceedings arising out of the same circumstances. For this reason, in the event that you conclude that any person has or may have acted improperly, your report should not identify such person by name, or refer to him or her in any manner as would enable them to be identified. If your consider that any person has acted in an egregious manner such as to require that his or her conduct ought to be brought to the attention of VFS, UKvisas or other body, you should consider, in consultation with the FCO Legal Adviser, how best this would be achieved, having due regard to the rights of all persons concerned.

21. As your report may address issues that could be the subject of subsequent legal, contractual or disciplinary proceedings, it should not state any conclusions of law or of legal liability.

22. Permission would be required from the Foreign Secretary, to be obtained via the FCO Legal Adviser, before holding interviews with the media, taking part in radio or television programmes, writing letters for publication in the press, or other public expression drawing on your role as Independent Investigator.

Administrative and Other Support, Payment and Costs

23. VFS, UKvisas, and as appropriate the FCO more widely, will provide you with such assistance and support as you may request and would be reasonable in the circumstances. The administrative and other support that you will require to enable you to undertake the investigation efficiently may change as the investigation proceeds. In the first instance, the FCO Permanent Under-Secretary will make arrangements to meet your need for competent secretarial support, to operate out of the FCO, but independently of UKvisas, and, if you consider this necessary, by way of non-FCO postal and email addresses. You should be in contact with Alison Little, in the FCO Permanent Under-Secretary's office, to finalise these arrangements. We agree that, as in your role as the Independent Monitor, it would be appropriate for you to work from your home address, travelling to London or elsewhere as necessary.

24. At the outset of your investigation, you will wish to make contact with VFS and UKvisas for reports as to facts, as they see them, as well as for relevant IT and other information. You have indicated that you will need expert IT advice on the cause of any security breach and whether the steps taken subsequently have fully rectified any problem found. Following your initial contact with VFS and UKvisas, you will be better placed to assess what advice you require on this matter and from whom such advice may be best obtained. Without prejudice to your independent status, it would at that point be appropriate for you to consider this matter with Tony Mather, the FCO Chief Information Officer, who would be well placed to assist in identifying suitable, and independent, IT expertise. Costs management in respect of advice sought from any independent IT expert that may reasonably and appropriately be retained will mirror that in respect of independent legal advice described below.

25. In the event that your investigation leads you to consider that there has been any breach of data security that could have national security implications, this matter should be brought to the immediate attention of Andrew Noble, the FCO Security Management Director, with whom the need for further advice and action should be discussed and agreed.

26. You have indicated that you will need independent legal advice and proposed that you should use the solicitors who advised you in your then capacity as the Scottish Legal Services Ombudsman. We agree that legal advice may be necessary and that you should be free to seek such advice as may be reasonable and appropriate. Without prejudice to this, to ensure that costs do not spiral without notice or control, before you retain legal assistance, the FCO would expect to see a statement of proposed fee rates and retains authority to direct that an alternative source of independent legal advice be sought if these rates appear unreasonable. We would also require notification of legal costs incurred and projected at any point at which such costs approach successive multiples of £5.000.

27. The FCO will cover the costs of your investigation in the first instance, including of the administrative and other support that will be provided to you for this purpose. We will also reimburse you for expenses incurred, including in respect of any trips abroad that it may be necessary for you to undertake as part of the investigation, on submission of a claim form and receipts. Any costs or expenses incurred by the investigation in the form of fees payable to external advisers, such as IT consultants and lawyers, should be submitted for payment to Alison Little, in the FCO Permanent Under-Secretary's office, as appropriate at your discretion and direction to ensure that the FCO has proper notice of costs incurred.

28. For purposes of this investigation, you will be acting in the capacity of Independent Investigator, rather than as the Independent Monitor. For ease of arrangement, however, you

will continue to receive your salary as the Independent Monitor throughout the period of the investigation, such salary being construed as payment to you in your role as Independent Investigator on a pro rata basis.

29. These arrangements will not affect the terms and conditions of your appointment as the Independent Monitor, your role as Independent Investigator being taken for administrative purposes, including leave, pension and associated arrangements, as an element of your on-going role as the Independent Monitor.

Appendix B: Typical questions asked of visa applicants for a visit visa

Section 1. About you

1. Name: First name Family name/surname Other names
2. Date of birth
3. Sex Male Female
4. Place of birth
5. Nationality
6. Father's full name First name Family name/surname
7. Mother's full name First name Family name/surname

Section 2. Your family

1. Marital status. If married or separated, please give your spouse's full name. Where is your spouse now? What is your spouse's date of birth? What is your spouse's nationality? Is your spouse travelling with you?
2. Do you have any children? If yes: How many children do you have? Full name. Date of birth. Place of birth. Nationality. Which country do they currently live in? Are they are travelling with you?

Section 3. Where do you live?

1. Country. What is your permanent home address? House/Street City, Town or Village Postal/PIN Code, Home telephone number.
2. Can we contact you here during the application process? If yes, Please provide your current address House/Street City, Town or Village Postal/PIN code Home telephone number.
3. Do you have an e-mail address? If yes: E-mail address

Section 4. Passport information

1. Passport / travel document number
2. Date of issue
3. Date of expiry
4. Place of issue
5. Is this your first passport? If No: Please provide details of the last passport you held Passport number Place of issue. Where is this passport now?

Section 5. Your immigration history

1. Have you travelled outside your home country?
   If yes: please list the last 3 countries you have visited.
2. Have you visited the UK before? If yes, Please give the date and duration of your stay/s
3. Have you ever applied for a UK visa before? If yes, Where was the previous application made? When did you apply? What type of visa did you apply for? What was the outcome?
4. Have you ever been refused a visa for the UK**?** If yes: At which post were you refused? When did you apply? What type of visa did you apply for? Did you appeal against the decision? Does this application differ in any way from the previous one? Please explain how it is different.
5. Have you ever been refused entry to the UK or had your leave to remain/enter cancelled**?** If yes: Where were you refused entry or had your leave to enter/ remain cancelled?. Why

did it happen? When did this happen? Did you appeal against the decision? What was the outcome of the appeal?

6. Have you ever been deported, removed or otherwise required to leave the UK**?** If yes**:** When was the notice served on you? What type of notice was it? Deportation Order APP104 IS151A. Why were you required to leave? If you appealed against the decision please give the details.
7. Have you ever been refused a visa for another country**?** If yes**:** Which country refused your visa? When were you refused? What was the reason for the refusal
8. Have you ever been deported, removed or otherwise? When was this? Have you been required to leave another country**?** If yes**.** Where was this? What was the reason?
9. Do you have any criminal convictions in any country? If yes: What was the conviction for? Please give the date of conviction. Where were you convicted? What was your sentence?
10. Have you ever been concerned in the commission, preparation, organisation or support of acts of terrorism, either within or outside the United Kingdom or have you ever been a member of an organisation which has been involved in or advocated terrorism in furtherance of its aims? If yes: Please give the details.
11. Have you ever been concerned in the commission, preparation or organisation of genocide or crimes, including crimes against humanity and war crimes, committed in the course of armed conflict? If yes: Please give the details

Section 6. About your visit

1. How long do you intend to stay in the UK?
2. Why are you going to the UK?
3. When will you arrive in the UK?
4. Where will you stay in the UK? Hotel/B&B - Name of Hotel/B&B. With Friends or family - Name Address Telephone number Other - please explain and Include address and telephone number
5. How much money are you taking with you on your visit?
6. Are any other funds available to you to finance this visit? If yes: Please explain what additional funds are available to you.
7. Do you have any family in the UK? If yes: Relationship to you Name Address Telephone number

Section 7. Employment and finances

1. Are you Employed/Self employed/ unemployed? If employed/self employed. What is your present job? What date did you start this job? What is the name of the company? Address. Telephone number. What is your monthly income?
2. Do you receive any income from any source other than employment, including friends or family? If yes. Please detail the additional income.
3. Do you own any assets, for example property? If yes. Please give details of your assets

SECTION 12 - DECLARATION (for all applicants)

Data Protection Statement

The Foreign and Commonwealth Office is processing the personal data on this form and related data for the purposes of promoting and protecting the interests of the United Kingdom and its citizens abroad. The data may be disclosed to other UK Government Departments and public authorities.

Appendix C

The Information Commissioner's good practice note on outsourcing.

"This good practice note sets out what you need to do to comply with the Data Protection Act 1998 when you outsource the processing of personal information. Typical examples would include outsourcing your payroll function or customer mailings. It sets out which parts of the Act are important when outsourcing and provides some good practice recommendations.
It applies when you use an organisation to process personal information for you, but you keep liability for the information and full control over its use.

What does the Act require?
When you contract or arrange with someone to process personal information on your behalf you remain responsible for the processing. This means that you will be liable for breaches of the Act.

• Outsourcing to any organisation

The Act requires you to take appropriate technical and organisational measures to protect the personal information you process, whether you process it yourself or whether someone else does it for you. To decide what measures are appropriate you need to take into account the sort of information you have, the harm that might result from its misuse, the technology that is available and also what it would cost to ensure an appropriate level of security.
When you employ another organisation to process personal information for you, you must choose one that you consider can carry out the work in a secure manner and, while the work is going on, you should check that they are doing this. You must also have a written contract in place with them. This contract must:

• make sure they only use and disclose the personal data in line with your instructions; and

• require them to take appropriate security measures.

The contract must be in place regardless of where the other organisation is based.

• Outsourcing to an organisation outside the EEA

The Act requires that where personal information is transferred to any country or territory outside the European Economic Area there should be an adequate level of protection in place. If you outsource work on personal information to an organisation outside the EEA, for example, to a call centre based in Asia or a transcription service based in Africa, you will have to make sure that the information is adequately protected. This will apply to the method you use to send the information, as well as the work itself.
There are two relatively simple ways to do this.

• If you use an organisation based outside the EEA to act on your behalf, as long as there are appropriate security measures in place, it is likely that there will be adequate protection for personal information. This is because appropriate security measures, the selection of a reputable organisation and restrictions on use help ensure an appropriate level of protection for personal data. However, you need to be sure that the contract with the other organisation and its terms are enforceable in that country.

• You can also use the model contract clauses approved by the European Commission and the Information Commissioner for transfers to organisations acting on your behalf. These contract terms can be used independently or incorporated into your main contract with the organisation. These terms can be found on the European Union website at:

http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

These are only two of the ways of ensuring adequacy. Other ways exist depending on the particular circumstances of the transfer. You can find more information about these on our website (www.ico.gov.uk) or from our helpline on 01625 545745.

Good practice recommendations

These are good practice recommendations if you want to use an organisation to process personal data on your behalf.

• Select a reputable organisation offering suitable guarantees about their ability to ensure the security of personal data.

• Make sure the contract with the organisation is enforceable.

• Make sure the organisation has appropriate security measures in place.

• Make sure that they make appropriate checks on their staff.

• Audit the other organisation regularly to make sure they are 'up to scratch'.

• Require the organisation to report any security breaches or other problems.

• Have procedures in place that allow you to act appropriately when you receive one of these reports.

Version 1.0 03.04.06"

Appendix D

Chief Information Officer in the Foreign and Commonwealth Office: role and remit

The position was created with effect from 1 April 2007 and heads up the Information & Technology Directorate which was created by bringing together 4 previously disparate FCO teams - IT Strategy Unit (ITSU), the Information Management Group (IMG), the IT Security Advisors (ITSA - previously in Security Management Directorate (SMD)) and the PRISM team (the FCO Enterprise Resource Planning system). The position does not have direct responsibility for the Consular or UKvisas teams which have their own IT delivery capability.

Principal Responsibilities:

- To ensure the FCO's overall business strategy takes full advantage of the technologies available to deliver HMG's overseas strategic priorities as efficiently as possible, and to champion IT-enabled change in the FCO.
- To define and implement information and IT strategies in line with the FCO's strategy and objectives.
- To be responsible within the FCO for the *Transformational Government Strategy*, ensuring a joined up approach, developing the potential for shared services with other Government departments, and participating actively in the Chief Information Officers' Council.
- To deliver, on time and to budget, the FCO's next generation desktop system, Future Firecrest, the new high classification systems, and ensure the smooth and efficient performance of the FCO's overall IT infrastructure.
- To act as Senior Information Risk Officer and manage the information assurance function.
- To maintain strategic partnerships with FCO Services and private sector suppliers to ensure the successful and timely delivery of systems to FCO staff.
- To manage IT procurement activities to ensure the negotiation of new contracts or re-negotiation of existing ones to deliver best value for money.
- To manage IT budgets of £100-150 million per annum, to ensure best practice in risk and financial management, and the achievement of efficiency targets in the context of SR07.
- To manage the intelligent client, information strategy and information services teams within the FCO (70-80 staff), and ensure its staff have the technical, professional and project management skills to deliver results.
- To act as head of the IT and information professions in the FCO.
- To promote the FCO's reputation as an innovative user of IT to deliver more effective services to the rest of Government and to the public.

The Foreign & Commonwealth Office's Chief Information Officer's views on governance and best practice in relation to government entering into contracts with the private sector where personal data is processed

1. The contracting company should have its own establish internal Information Assurance standards (based on ISO 7799 security & ISO 9006 data protection act) and governance process that is applicable to all parts of its operation and compliance is audited on a regular basis with clear consequences for non-compliance.

2. These standards / governance processes should be made clear to the 3rd party as part of any tendering process and their ability to comply with them a pre-requisite to any award of contract.

3. If the service being contracted is already established then it should be audited (which should include site visits) to ensure compliance.

4. If the service is to be developed then it is critical that the contracting company security team is engaged at the start of the development process to ensure that compliance is built into the service rather than bringing them in at the end and trying to retro fit. This involvement should be a clear part of the development plan.

5. Compliance to the standards should be tested and be one of the 'go-live' criteria.

6. There should be regular testing of the external services to ensure ongoing compliance and to help prevent any breaches in security.

7. It is not unusual to have contractual penalties attached to failure in compliance.

Appendix E Acknowledgements

This investigation was set up at short notice, and with a relatively tight reporting deadline. The timetable has, however, been helpful because it ensures that lessons can be quickly learnt and any necessary remedial action taken without delay.

I could not have completed this report without willing co-operation and help from a number of sources, for which my thanks;

- UKvisas and VFS have been open-minded, accessible and courteous. The evidence I requested, whether on paper or orally, was provided willingly and promptly. Neither has been unduly defensive and this positive attitude meant that a great deal could be covered in a short space of time.

- I met a range of organisations and Government officials, all of whom made themselves available and discussed their roles with real enthusiasm.

- My legal advisers and independent IT experts provided valuable comment and opinion on matters in which I do not have specific expertise. I am also especially grateful to the Office for Government Commerce who undertook a significant piece of work for me, condensing it into a sharply focused report.

- The Office of the Permanent Under Secretary of State at the Foreign & Commonwealth Office provided me with an independent office, and, most important of all, a highly efficient Administrative Assistant who equipped the office and then handled a significant amount of papers and day to day contacts. I could not have managed without her.