Foreign & Commonwealth Office response to recommendations contained in the *Report of the Independent Investigation: breach of data security in the VFS online UKvisas application facility, operated through VFS websites in India, Nigeria and Russia*

Recommendation: *I recommend that the VFS online application system should not be re-opened, though I note UKvisas has already reached that decision. (para 158)*

Accepted. The VFS websites will not be reopened. They will be replaced by visa4UK, the UKvisas online visa application facility. This is and will continue to be the only online application system used by UKvisas**.**

Recommendation: *UKvisas has agreed an action plan with the ITSA* [Foreign & Commonwealth Office IT security advisors]. *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. (para 159)*

Accepted. visa4UK was reviewed by the FCO's IT Security Advisers in 2003, 2004 and 2005. UKvisas has now implemented the key recommendations and agreed with ITSA a timetable for further security testing over the months ahead. Where these tests identify the need for changes to visa4UK, UKvisas will agree with ITSA a timetable for implementation – with changes prioritised on the basis of urgency, feasibility and cost. The UKvisas Chief Information Officer (see below) will ensure that the process is robust and transparent.

Recommendation: *I recommend that, so far as is possible with the limited material available, UKvisas should continue to ask CESG* [part of Government Communications Headquarters, GCHQ] *to assist in analysing the logs for evidence of unauthorised access. (para 161). I recommend that UKvisas should continue its series of checks to try to ascertain if there has been unauthorised use of personal data.* (*para 162*)

Accepted. UKvisas will consult CESG to ascertain whether any further checks can be made. UKvisas will also task Risk Assessment Officers in India, Nigeria and Russia to conduct further checks. And UKvisas will continue to monitor complaints and media logs for any evidence of unauthorised use of personal data.

Recommendation: *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. (para 164)*

Accepted. The new contracts concluded in February 2007 do contain detailed provisions on data protection including a Security Schedule requiring Commercial Partners to comply with ISO17799 (Code of Practice for Information Security Management), ISO27001 (Information Security Management – Specification with Guidance for Use) and good industry practice. Before opening a Visa Application Centre, the Commercial Partners must demonstrate their compliance with the Security Schedule – including independent assessments of the security of the premises and the security of their IT systems. All this is captured in a "Security Milestone Map" prepared by the Commercial Partner for monitoring by UKvisas and review at the monthly Security Management Forum set up as part of the new contract governance structure.

If a security incident occurs, under the new contract the Commercial Partner is required to report it immediately to UKvisas. They must also investigate the incident, carry out corrective action, document the results and provide a copy to UKvisas. UKvisas has the right to inspect all security aspects of the Commercial Partners' operations to verify the measures in place.

UKvisas is undertaking a strategic review of data processing (including by Commercial Partners), in order to strengthen Data Protection Act risk management processes. In addition, we will carry out a detailed audit of Commercial Partners' data security procedures and practice in the light of this Report, to reinforce its findings and ensure that they have been understood and implemented. We will take advice on whether the existing contractual provisions need supplementing with further operational guidance for Commercial Partners and overseas Posts, particularly in relation to monitoring their compliance with the Data Protection Act. UKvisas will shortly issue targeted guidance on the 8 Data Protection Act principles for overseas Posts. Staff training is also being updated to reflect the wide range of Data Protection Act issues faced by the business. This will form part of the wider arrangements UKvisas is introducing to ensure full compliance with Foreign & Commonwealth Office Data Protection Act procedures and IT Security Policy (see below).

Recommendation: *Governance of information assurance needs to be held at Board level, and I recommend that UKvisas Board includes a member with that specific responsibility. (para 172)*
I recommend that the Foreign & Commonwealth Office's CIO's [Chief Information Officer] *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. (para 174)*

Accepted. The UKvisas Corporate Services Director – who is a member of the UKvisas Board - will assume the role of Chief Information Officer for UKvisas. She will participate as appropriate in governance structures established by the Foreign & Commonwealth Office's Chief Information Officer, who is a member of the main Foreign & Commonwealth Office Board. A UKvisas Technical Design Authority will also be established, reporting to the UKvisas Chief Information Officer, to ensure the overall coherence and integrity of UKvisas' business processes. The Technical Design Authority will be responsible for ensuring that UKvisas complies with Foreign & Commonwealth Office Data Protection Act procedures and IT Security Policy.

UKvisas is accountable to the Foreign & Commonwealth Office Chief Information Officer in his capacity as the Department's Senior Information Risk Officer – including compliance with Foreign & Commonwealth Office Data Protection Act procedures and IT Security Policy. UKvisas retains direct responsibility for delivery of the IT systems it uses but works in close co-operation with the Foreign & Commonwealth Office's CIO and his team. The UKvisas Chief Information Officer will review the current governance arrangements with the Foreign & Commonwealth Office's Chief Information Officer to ensure they are fit for purpose.

Recommendation: *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. (para 167)*

Accepted. UKvisas accepts that a fundamental lesson arising from the Report is that there has to be adequate oversight of commercial partners' performance, based on a sound contractual arrangement, now in place, and also on expert advice and well-resourced internal management functions. UKvisas agrees that it holds ultimate responsibility for the security of visa applicants' personal data and that this has to be a central aspect of business process, not an add-on. The establishment of a UKvisas Chief Information Officer role and Technical Design Authority will clarify responsibilities for information handling. UKvisas is also strengthening its arrangements, beyond data security issues, for the setting of

core operating standards, reporting on their implementation and dealing with any issues arising. This will be done through the Business Assurance Project.

Recommendation: *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. (para 169)*

Accepted. We are revising our procedures so that complaints are investigated thoroughly and uniformly throughout the business and – where possible – resolved to the satisfaction of all parties. The procedures will be clear, transparent, and aligned with those of our commercial partners. A key point will be the early identification, escalation and handling of business critical complaints. The management of complaints raised with UKvisas by 3rd parties will complement the monitoring of internal risks and issues through the Business Assurance project.

Recommendation: *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. (para 170)*

Accepted. Letters will be sent to Mr Mitra and Mr Winder during the week commencing 30 July 2007.

Recommendation: *The Government's Chief Information Officer provided me with outsourcing governance notes and I commend them (para 175)*

Accepted. The new contracts with Commercial Partners do respect these guidelines. We shall re-validate their implementation when we carry out the audit referred to above.