

**21 November 2007**

**For immediate release**

## **LSE Identity Project Summary Briefing about Security Concerns relating to the National Identity Register**

### **Introduction**

Following yesterday's announcement in Parliament that personal data about 25 million individuals has gone missing<sup>1</sup>, a number of commentators have highlighted the similarities between the records held by HMRC about recipients of child benefit and the proposals to hold details about all UK citizens on the National Identity Register as part of the Identity Cards Scheme. The purpose of this LSE Identity Project briefing is to review the ongoing concerns with the security of the NIR.

### **Initial plans**

Whilst Parliament was debating the Identity Cards Bill (May 2005–March 2006) the design of the Identity Cards Scheme was based on the creation of a database that would hold all the identity data (biographical data, biometric data and security / administrative data) in this single (logical) database.

The security of this design was one of the issues addressed by the LSE Identity Project's *main report* issued in June 2005<sup>2</sup>. The chapter on security was written by a British Nato and defence specialist<sup>3</sup> and warned of the threats posed by having a single, central repository for all personal data. The chapter concluded that "the National Identity Register poses a far larger risk to the safety and security of UK citizens than any of the problems that it purports to solve"<sup>4</sup>.

In light of these concerns, the LSE proposed an alternative blueprint for a National Identity Scheme. One of the key characteristics of this alternative was that it sought to federate the storage of this personal information so that it would not be possible for all the identity data held on the NIR to be disclosed in any one activity (i.e. it would not be possible to copy all the data held on the NIR onto CDs even if any individual had appropriate security clearance to undertake such an activity).

---

<sup>1</sup> Alistair Darling, Hansard 20 November 2007 : Column 1101

<sup>2</sup> <http://identityproject.lse.ac.uk/identityreport.pdf> Chapter 14

<sup>3</sup> Hencke, D., & Dodd, V. (2006). Defence expert undermines Blair on safety of ID cards. The Guardian. Archived at <http://www.guardian.co.uk/idcards/story/0,,1708461,00.html>

<sup>4</sup> P. 187

In August 2005, the Home Office issued its response to the LSE alternative blueprint<sup>5</sup>, restating its argument for a 'centralised approach' to data storage:

**We will provide more secure storage of your information:**

Instead of allowing data to be stored in several distributed "data backup sources" operating with different levels of security controls, data storage operations will be in a small number of highly secure environments. These would be staffed by security vetted specialists who would be subject to maximum security working processes involving segregation of role and comprehensive audit trail functionality<sup>6</sup>.

They also argued that their approach was 'common sense': "For example, a bank or supermarket does not leave small amounts of cash in its tills overnight; it transfers this cash to a safe—a highly secure central environment. This is more cost-effective than making every individual till as secure as the safe"<sup>7</sup>. The Home Office continued by arguing that this approach "complies with industry best practice"<sup>8</sup>.

When members of the Identity Cards Project Team appeared before the House of Commons Science and Technology Select Committee in March 2006, Nigel Seed (Project Director, National Identity Register and Operational Technology Infrastructure) told the Select Committee: "Security is not going to be an add-on, it is being done now. We have not even gone out with our requirements. The security is embedded within my procurement team. ... The security of the data centre itself is down to even very basic things like making sure it is not on or near a floodplain. We are looking at all that sort of stuff, right from very basic level access and flooding and losing it that way right the way through to hacking"<sup>9</sup>.

## **Strategic Action Plan**

In December 2006, UKIPS released its 'Strategic Action Plan' that sought to reduce the risks and costs of the Scheme<sup>10</sup>. The plan acknowledged that biographical, biometric and administrative / security information "do not all need to be held in a single system. In fact, for security reasons, and to make best use of the strengths of existing systems, it makes sense to store them separately". The plan proposed that each aspect be stored on its own (existing) database. Thus, biographical information would be stored on the Department of Work and Pensions Customer Information

---

<sup>5</sup> [http://identityproject.lse.ac.uk/HomeOffice\\_ResponseTo\\_LSE\\_AlternativeBlueprint.pdf](http://identityproject.lse.ac.uk/HomeOffice_ResponseTo_LSE_AlternativeBlueprint.pdf)

<sup>6</sup> P. 5 of PDF

<sup>7</sup> P. 5 of PDF

<sup>8</sup> P. 5 of PDF

<sup>9</sup> Answer to Q344

<sup>10</sup> [http://www.ips.gov.uk/identity/downloads/Strategic\\_Action\\_Plan.pdf](http://www.ips.gov.uk/identity/downloads/Strategic_Action_Plan.pdf)

System, biometric data on existing biometric databases and the Public Key Infrastructure on existing passport office systems<sup>11</sup>.

However, whilst this model allows biographical information to be kept separate from biometric information it is still based on the idea of a single (logical) database that holds the biographical information of *all* individuals registered with the Scheme, in the same way as the HMRC database stored details of *all* Child Benefit recipients.

## **Procurement**

In August 2007, UKIPS announced the launch of its National Identity Scheme Strategic Supplier Framework<sup>12</sup>. This is the “procurement of a framework arrangement to provide capabilities to support the National Identity Scheme. ... The procurement approach will select a small group of the best suppliers in the market for the required services. These suppliers will work with IPS and its partner agencies to deliver capabilities for the Scheme”<sup>13</sup>.

Following this announcement, eleven responses were received and eight suppliers were shortlisted<sup>14</sup>. These companies have been invited “to participate in Competitive Dialogue with IPS over the coming months prior to seeking final tenders for the framework arrangement”.

## **Next steps**

At the time of writing, it is unclear what effect the Child Benefit data breach is having on political support for the more controversial aspects of the National Identity Scheme (e.g. single central register of personal data, detailed audit trail of identity verification activities against the Register, data accumulation to support the biographical footprint check as part of the enrolment process<sup>15</sup>) as opposed to the less controversial aspects of improving the quality of the passport issuing process.

However, with the shortlisted companies participating in a competitive dialogue with UKIPS at this time, there is a clear opportunity for the procurement process to re-emphasize security aspects of the Scheme (both technological and administrative).

---

<sup>11</sup> Pp. 10–11

<sup>12</sup> <http://www.ips.gov.uk/identity/working-suppliers-framework.asp>

<sup>13</sup> <http://www.ips.gov.uk/identity/working-suppliers-framework.asp>

<sup>14</sup> Accenture; BAE Systems; CSC; EDS; Fujitsu; IBM; Steria; and Thales

<sup>15</sup> E.g. our submission to the Home Affairs Select Committee Inquiry into “A surveillance society?” [http://identityproject.lse.ac.uk/LSE\\_HAC\\_Submission.pdf](http://identityproject.lse.ac.uk/LSE_HAC_Submission.pdf)

Moreover, as we have argued on a number of occasions<sup>16</sup>, if the government is to retain any public confidence in the Scheme, the process of evaluating the security aspects of procurement must be undertaken in a spirit of openness and transparency (and not one of desperate secrecy as has been the case with the Office of Government Commerce Gateway Reviews of the Scheme<sup>17</sup>).

## **Recommendations**

- ✍ We recommend that the Home Office and the Cabinet Office hold *open* meetings with industry and academic experts, as well as consumer and civil liberties groups, to discuss the security considerations in the Scheme in light of recent events;
- ✍ We also recommend that those aspects of the procurement process that relate to aspects of the Scheme that affect the security of personal data be placed on hold until these experts and groups have openly reviewed these security considerations;
- ✍ Finally, we recommend that the Home Affairs Committee explicitly consider the challenges for transformational government and individual privacy that arise from the widespread use of centralised databases.

For LSE research and reports on identity policy please see <http://identityproject.lse.ac.uk>

---

<sup>16</sup> E.g. <http://identityproject.lse.ac.uk/CJM2007.pdf>, <http://identityproject.lse.ac.uk/s37response.pdf> p. 17, <http://identityproject.lse.ac.uk/s37Response2.pdf> p. 17.

<sup>17</sup> See, for example, <http://www.computerweekly.com/Articles/2007/05/31/224457/ogc-heads-for-high-court-to-guard-results-of-gateway-review-on-id.htm>