House of Commons

Science and Technology Committee

Identity Card Technologies: Scientific Advice, Risk and Evidence

Sixth Report of Session 2005–06

HC 1032

House of Commons

Science and Technology Committee

Identity Card Technologies: Scientific Advice, Risk and Evidence

Sixth Report of Session 2005–06

Report, together with formal minutes, oral and written evidence

Ordered by The House of Commons
to be printed 20 July 2006

HC 1032
[Incorporating HC 900-iii, v and xi]
Published on 4 August 2006
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

The Science and Technology Committee

The Science and Technology Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Office of Science and Innovation and its associated public bodies.

Current membership

Mr Phil Willis MP *(Liberal Democrat, Harrogate and Knaresborough)(Chairman)*
Adam Afriyie MP *(Conservative, Windsor)*
Mr Jim Devine MP *(Labour, Livingston)*
Mr Robert Flello MP *(Labour, Stoke-on-Trent South)*
Dr Evan Harris MP *(Liberal Democrat, Oxford West & Abingdon)*
Dr Brian Iddon MP (*Labour, Bolton South East*)
Margaret Moran MP *(Labour, Luton South)*
Mr Brooks Newmark MP *(Conservative, Braintree)*
Anne Snelgrove MP *(Labour/Co-op, South Swindon)*
Bob Spink MP *(Conservative, Castle Point)*
Dr Desmond Turner MP *(Labour, Brighton Kemptown)*

Powers

The Committee is one of the departmental Select Committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No.152. These are available on the Internet via www.parliament.uk

Publications

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the Internet at www.parliament.uk/s&tcom
A list of Reports from the Committee in this Parliament is included at the back of this volume.

Committee staff

The current staff of the Committee are: Chris Shaw (Clerk); Celia Blacklock (Second Clerk); Dr Hayaatun Sillem (Committee Specialist); Dr Anne Hicks (Committee Specialist); Ana Ferreira (Committee Assistant); Robert Long (Senior Office Clerk); and Christine McGrane (Committee Secretary).

Contacts

All correspondence should be addressed to the Clerk of the Science and Technology Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 2793; the Committee's email address is scitechcom@parliament.uk

Contents

Report

Summary

This Report is the final of three case studies considering the Government's treatment of scientific advice, risk and evidence. It focuses upon the Home Office's identity cards scheme, which uses various technologies including biometrics, information and communication technology (ICT) and smart cards. We considered this scheme in order to explore the ways in which scientific advice, risk and evidence could be managed in relation to technologies that are continually developing.

This inquiry has found several areas in which the Home Office's treatment of scientific advice and evidence appears to be following good practice: the establishment of advisory committees, the use of Office of Government Commerce (OGC) Gateway Reviews and the development of risk management strategies are examples. We welcome the Home Office's commitment to implementing the scheme gradually rather than using a "big bang" approach, which could jeopardise the success of the programme.

We have also identified weaknesses in the use of scientific advice and evidence. We are disappointed with the lack of transparency surrounding the incorporation of scientific advice, the procurement process and the ICT system. Potential suppliers are confused about the extent to which the scheme will be prescriptive and when technical specifications will be released. Whilst the Home Office has attempted to consult the wider community, stakeholders have complained that consultations have been unduly limited in scope and their objectives have been unclear. As a result, the wider community does not have the level of confidence in the scheme that could reasonably be expected at this stage. Whilst the Home Office has determined some aspects of the scheme such as the biometrics, it has left other aspects such as the structure of the database undetermined. Its decisions demonstrate an inconsistent approach to scientific evidence and we are concerned that choices regarding biometric technology have preceded trials. Given that extensive trialling is still to take place, we are sceptical about the validity of costs produced at this stage. We note the danger of cost ceilings driving the choice of technology and call for the Home Office to publish a breakdown of the technology costs following the procurement process.

The identity cards scheme has at least another two years before identity cards begin to be introduced and the scheme has not yet entered its procurement phase. There is still time for the Home Office to make alterations to its processes. We encourage the Home Office to seek advice on ICT from senior and experienced professionals and to establish an ICT assurance committee. Whilst biometric technology is an important part of the scheme, it must not detract from other aspects of the programme, in particular ICT. It is crucial that the Home Office increases clarity and transparency across the programme, not only in problem areas. We also emphasise that if evidence emerges that contradicts existing assumptions, changes must be made to the programme even if the timescale or cost of the project is extended in consequence.

1 Introduction

Scientific advice to Government inquiry

1. The Committee announced a broad inquiry into the handling of scientific advice, risk and evidence in policy-making in November 2005.[1] As part of this inquiry, the Committee chose to focus on three case studies considering the EU Physical Agents (Electromagnetic Fields) Directive, the classification of illegal drugs, and the technologies supporting the Government's identity card proposals. The lessons learnt in the case studies will feed into the general conclusions drawn in the over-arching report from the broad inquiry.

2. The Committee chose to focus on the role of scientific advice, use of evidence and handling of risk within the identity cards programme for several reasons. First, the identity cards programme provided a case study that concentrated on a technology-driven policy. The scheme critically involves more than one technology, which increases its interest. Secondly, the programme uses technologies that are continually developing and in this context, the ongoing need for scientific advice and evidence is particularly important. Finally, the inquiry was particularly timely given the contemporaneous passage of the Identity Card Bill through the House.

3. The identity cards scheme is a major project that will use information and communication technology (ICT) and biometric technologies in recording, holding and verifying personal identity information. As such, it is reliant upon sound scientific advice and requires an appropriate approach to the handling of risk. The cost of failure of this project would be enormous, both financially and politically in terms of public trust.

4. In the course of our inquiry we held three oral evidence sessions and took evidence from the following:

a) Ms Katherine Courtney, the then Director of the Home Office identity cards programme; Dr Henry Bloomfield, the then Technical Lead in the identity cards programme; Mr Nigel Seed, the then Project Director of the National Identity Register and Operational Technology Infrastructure, and Mr Marek Rejman-Greene, Head of the Home Office Biometrics Centre of Expertise;

b) Nick Kalisperas, Director of Markets at Intellect; Jerry Fishenden, National Technology Officer at Microsoft; Dave Birch, Director of Consult Hyperion; Professor Martyn Thomas from the UK Computing Research Committee (UKCRC); Dr Tony Mansfield from the National Physical Laboratory (NPL); Dr John Daugman, Reader in Computer Vision and Pattern Recognition at the University of Cambridge; Dr Edgar Whitley, Reader in Information Systems at the London School of Economics (LSE), and Professor Angela Sasse, Professor of Human-Centred Technology at University College London (UCL); and

c) the Parliamentary Under-Secretary of State for nationality, citizenship and immigration, Home Office, Joan Ryan MP.

1 www.parliament.uk/parliamentary_committees/science_and_technology_committee/scitech091105.cfm

5. The transcripts of these sessions are published with this Report, along with the 19 written submissions we received in response to our call for evidence and as answers to supplementary questions. We also held informal meetings with the Department of Homeland Security, the International Biometrics Group and Ultra-Scan during our visit to the United States in March 2006. In July, the Chairman held a private meeting on risk management with Katherine Courtney, Executive Director of Business Development and External Affairs at the Identity and Passport Service (IPS), Dr Henry Bloomfield, Technical Lead, National Identity Register and Operational Technology Infrastructure at the IPS, and Catherine Kimmel, Risk Manager at the IPS. We would like to place on record our thanks to all those who contributed to this inquiry, by giving evidence or by assisting us on our visit. We would also like to thank our specialist adviser, Professor Brian Collins, Head of the Department of Information Systems, Defence College of Management and Technology, Cranfield University.

2 Background

The Identity Cards Scheme

6. Identity cards were compulsory in the United Kingdom from 1939 to 1952 under the National Registration Act 1939, acting as a security measure during the war and aiding rationing following the war. After the National Registration Act was repealed in October 1951, identity cards were no longer used. In the following years various proposals for identity cards were made, including a Green Paper on identity cards in May 1995.[2] Following a Report from the House of Commons Home Affairs Committee in 1996, the Government announced that it intended to introduce a voluntary identity card scheme.[3] The Government's plans to introduce a draft Bill in the 1996–97 Session of Parliament were cut short by the May 1997 General Election.

7. The notion of an identity cards scheme was reintroduced by the then Home Secretary, Rt Hon David Blunkett MP in February 2002.[4] The Home Office ran a consultation on entitlement cards and identity fraud from July 2002 until January 2003.[5] In November 2003, the Government published its plans for identity cards as *Identity Cards: the Next Steps.*[6] Five months later in April 2004, the Government published a draft Bill and launched a consultation on the draft legislation.[7] Following a Report by the House of Commons Home Affairs Committee in July 2004, the Government introduced an Identity Cards Bill into the House of Commons in November 2004.[8] This Bill fell at the dissolution of Parliament in April 2005. A new Identity Cards Bill was introduced on 25 May 2005 and it was finally given Royal Assent on 30 March 2006.

8. The Identity Cards Act 2006 outlines the main aims of the scheme as maintaining a secure and reliable record of facts about individuals in order to:

- prevent or detect crime;
- ensure national security;
- enforce immigration controls;
- secure the efficient and effective provision of public services; and
- enforce prohibitions on unauthorised working or employment.[9]

2 Home Office, *Identity Cards: a consultation document,* Cm 2879, May 1995

3 Home Affairs Committee, Fourth Report of Session 1995–96, HC 172–I; Home Office, *The Government Reply to the Fourth Report from the Home Affairs Committee,* Session 1995–96, Cm 3362, August 1996

4 HC Deb, 7 February 2002, col 1028

5 Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*¸ Cm 5557, July 2002

6 Home Office, *Identity Cards: The Next Steps,* Cm 6020, November 2003

7 Home Office, *Legislation on Identity Cards: A Consultation,* Cm 6178, April 2004

8 Home Affairs Committee, Fourth Report of Session 2003–04, *Identity Cards,* HC130–I

9 *Identity Cards Act 2006,* para 1(3–4)

Overview of Events

July 2002	Home Office launches consultation on entitlement cards and identity fraud
January 2003	Home Office consultation ends
November 2003	Government response to consultation findings Home Office publishes *Identity Cards: Next Steps*
April 2004	Government published draft bill on identity cards and launches consultation on draft bill
July 2004	House of Commons Home Affairs Committee Report on Identity Cards, Fourth Report of Session 2003–04, HC 130
October 2004	Government Response to Home Affairs Committee Report
November 2005	Presentation and first reading of original Identity Cards Bill
April 2005	Identity Cards Bill falls at dissolution of Parliament
May 2005	Introduction of new Identity Cards Bill
March 2006	Identity Cards Bill receives Royal Assent
April 2006	Creation of Identity and Passport Service

9. The Act requires all individuals over the age of 16 to register details such as their identity, address, residential status and biometric information including fingerprints or iris scans.[10] As part of the application process, individuals will be asked to visit a local or mobile centre in order to check their biographical details and to record their biometrics. This enrolment process will be overseen by individuals trained in operating the machines necessary to record biometric information. These details will be stored on a National Identity Register (NIR) and on ID cards that are issued to individuals. This information can then be used by accredited organisations to verify an individual's identity.

10. The first identity cards are expected to be issued in 2008 but the Home Office has continually emphasised that the timetable is flexible, in accordance with Office of Government Commerce guidelines.[11] Katherine Courtney, the then Director of the identity cards programme, stated in oral evidence to the Committee that "Our plans have always been to take an incremental implementation to this in a step-by-step way, building on other developments and rolling out over a period of time".[12] Furthermore, she noted that "we have always said that the ready-for-service date for this system would be dependent on the solution that industry proposes to us during the procurement process".[13] In response to questions regarding reports of an "early variant" card using a facial image or two fingerprints, the Home Office wrote:

10 Some individuals will be excluded such as those who are residing in the UK without an entitlement to remain there. *Identity Cards Act 2006*, para 1–2.

11 Ev 112

12 Q 310

13 Q 328

> "the term 'early variant' is misleading in implying that there are firm plans for a different type of card to be issued earlier than others. The plans for ID cards have always been incremental with no 'big bang' implementation and the Identity and Passport Service is considering the most appropriate first incremental steps to introduce ID cards."[14]

The Home Office admitted that the timetabling of the programme was being reviewed by the IPS but said that it "remains committed to delivering the ID cards programme as soon as possible, starting with biometric residence permits for foreign nationals in 2008" (see paragraph 41).[15]

11. The identity cards scheme is closely related to several other Home Office projects. Katherine Courtney explained to us on 22 March 2006 that:

> "We have the biometric visas rolling out over the next year or two years, we have biometric residence permits rolling out and we have the biometric passports. We introduced the first electronic passport only this month, that was when the first one rolled off the production line. All of these things are testing the technologies that are the building blocks for this scheme."[16]

Biometric passports, including chips with the holder's facial biometric, were introduced in March 2006.[17] These passports are in line with the standards set by the International Civil Aviation Organisation (ICAO) in May 2003, which nominated facial recognition as the primary biometric with iris and fingerprint as backup.[18]

Management

12. In order to deliver the scheme, the Home Office has created an Identity and Passport Service (IPS) incorporating the United Kingdom Passport Service (UKPS) and the Home Office's identity cards programme team. This new service became operational on 1 April 2006 and the outline management structure for the agency is shown in Figure 1 below. As a result of these changes, the members of the identity card programme team that gave oral evidence to us on 22 March 2006 have now got new job titles. Katherine Courtney is no longer the Director of the identity cards programme but the Executive Director of Business Development and External Affairs. Nigel Seed is Director, NIR and Operational Technology Infrastructure and Dr Henry Bloomfield is Technical Lead, NIR and Operational Technology Infrastructure. In the remainder of this Report, when referring to these individuals we will use their new job titles.

14 "Emails from Whitehall officials in charge of ID cards", *The Sunday Times,* 9 July 2006; Jean Eaglesham, "ID cards procurement put on hold", *The Financial Times,* 12 July 2006, p 2; Ev 129

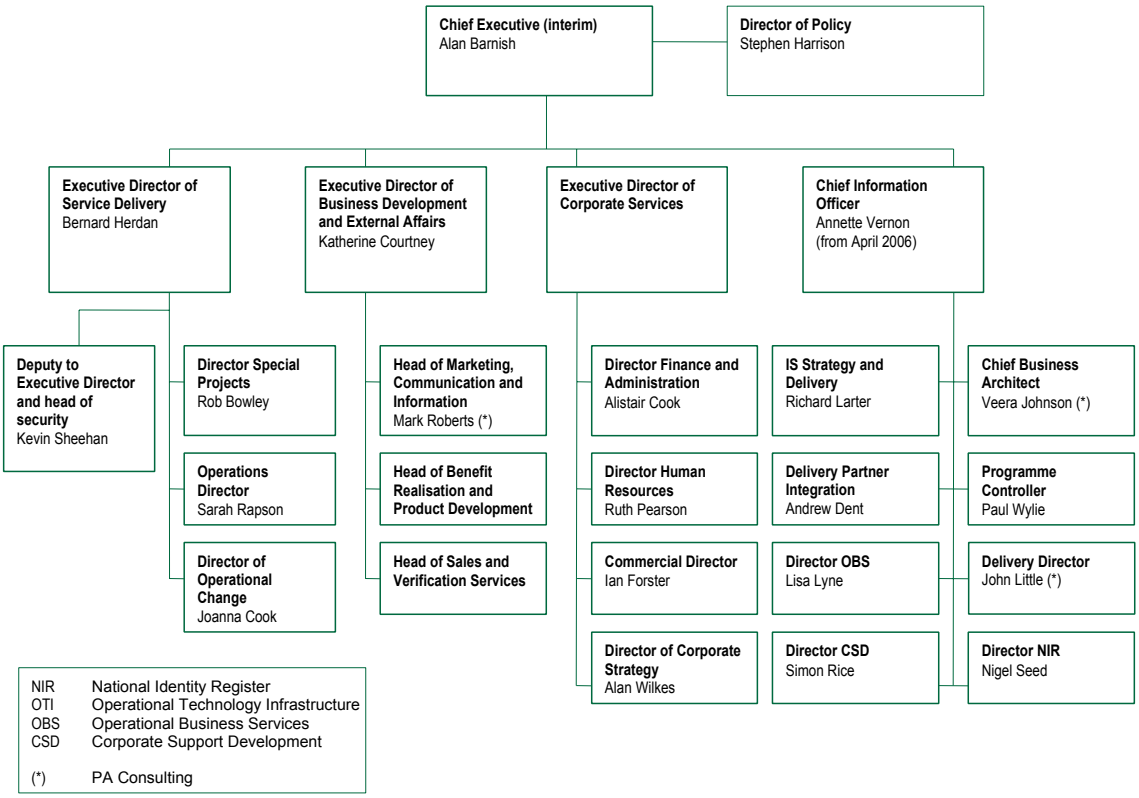
15 Ev 129

16 Q 371

17 "UK to issue its first biometric passports", *Western Mail*, 6 March 2006, p 10

18 http://www.icao.int/mrtd/biometrics/recommendation.cfm

Figure 1 Senior Management Structure for the Identity and Passport Service



Source: Government Memorandum, Appendix 2, Ev 53

13. The new service will be headed by a Chief Executive who will be recruited through open competition. The Chief Executive will also have a role within the Home Office as Director General Identity Services and will sit on the Home Office's Group Executive Board.[19] As such we have been assured that the procedures and facilities in place for the Home Office with regard to scientific advice will remain available to the Identity and Passport Service.[20]

14. The Home Office told us that as of February 2006 there were 186 people working with the identity cards programme team: 54 civil servants, 98 consultants and 34 interims. Since the creation of the IPS, the Home Office has said that the number of people working on the identity cards programme has not changed significantly. As Figure 1 shows, the Head of Marketing, the Chief Business Architect and Delivery Director within the IPS are consultants from PA Consulting. In 2004, the Home Office announced that PA Consulting had won a contract to aid the implementation of the identity card programme.[21] The contract commenced in May 2004 and lasts up to a maximum of three years. Between 6 April 2005 and 18 April 2006, the Home Office paid PA Consulting £14,248,799.21 for work on the identity cards programme.[22] The Home Office said that it was necessary to

19 Ev 118

20 As above

21 "ID cards-Home Secretary announces private sector partner", Home Office press release 196/2004, 24 May 2004

22 HC Deb, 18 April 2006, Col 448W

involve a private company because it did not have "ready access to certain skill sets and resources necessary for implementation of a large and complex project such as Identity Cards".[23] The Home Office responded to questions from us regarding the role of PA Consulting by explaining that:

> "PA support the design, feasibility testing, security accreditation, business case and procurement elements of the proposed scheme. The specialist skills include project and programme management, procurement, smart cards and biometrics, business process design, financial modelling and business case development."[24]

Overview of proposed technology

Biometrics

15. The Identity Cards Act 2006 states that biometric information will be recorded in the National Identity Register. The Act defines biometric information in relation to an individual as "data about his external characteristics, including, in particular, the features of an iris or of any other part of the eye".[25] There are many different types of biometric technology: facial, fingerprint, iris, signature, voice, hand geometry, vascular patterns, retina, DNA, ear recognition, keystroke and gait. The Government has stated that for ID cards it intends to develop a multi-modal scheme using 13 biometrics: 10 fingerprints, two irises and one face.[26] The Home Office has decided to use multiple biometrics for two key reasons. Firstly, it will ensure that as high a proportion of the population can enrol as possible. For example if an individual is missing a hand, they will still be able to enrol on iris or face. Secondly, if any problems occur during the verification process, for example with fingerprints, then it will be possible to double-check with iris scanning.[27] However, it is envisaged that different biometrics would be used for different scenarios. Katherine Courtney, the Executive Director of Business Development and External Affairs at IPS, explained in oral evidence that "In different business applications, a different biometric might be more appropriate than others. You see, for instance, iris being used quite successfully where you have a high volume of people passing through a system, such as the expedited gate clearing at the airports".[28]

16. Biometric systems work by converting a captured image into a template, which can be used in different ways. A one-to-one match can compare the biometrics to a template obtained on a previous occasion. A one-to-many search looks for a match for the biometric in a database of templates, which takes longer. The Government is proposing that the templates be stored on the National Identity Register and on a chip in the identity card. The biometrics will therefore link an individual both to their card and to the Register. In evidence to the House of Commons Home Affairs Committee, the then Home Secretary

23 Ev 75

24 As above

25 *Identity Cards Act 2006,* para 42(1)

26 HC Deb, 13 February 2006, Col 1209

27 Q 297

28 Q 292

David Blunkett said that "the moment someone presents the same biometric but with a different identity, a different name and presentation, that would automatically show up as already existing on the database".[29]

17. The accuracy of biometric systems depends on a number of basic performance measurements:

a) False match rate—the probability that a person's biometric matches the enrolment template of another person.

b) False non-match rate—the probability that a person's biometric fails to match their own enrolment template.

c) Failure to acquire rate—the submitted image is too poor for the system to make a reliable decision. Failure to acquire occurs for several reasons: when the enrolment environment is unsuitable, physical problems presenting the biometric eg. arthritis, or where the biometric is missing (approximately 1 person in 70,000 does not have an iris due to the inherited condition 'aniridia' and over 1 in 1000 fingers are missing or have no fingerprint due to scar tissue). [30]

18. There are no mutually-accepted standards for testing biometric technology and industry claims about performance vary widely. Most independent testing of biometric technologies has been undertaken by the National Physical Laboratory (NPL) in the UK and the National Institute for Standards and Technology (NIST) in the United States. Although there are several schemes that use biometric technology, there is very little published information from real life deployments.[31] The Home Office has stated that it expects the following performance levels to be sufficient for its requirements in the identity cards scheme:[32]

- Face—failure to acquire rate close to zero, a false accept rate of 1%.
- Fingerprint—failure to acquire rate of 0.5-1%, false match rate of 1.3e-10, false non-match rate of 0.01.[33]
- Iris—failure to acquire rate of 0.5%, false non-match rate of 5 % false match rate of 5e-12.[34]

29 Home Affairs Committee, Fourth Report of Session 2003–04, *Identity Cards,* HC 130–I, p 44

30 Tony Mansfield & Marek Rejman-Greene, *Feasibility Study on the Use of Biometrics in an Entitlement Scheme*, February 2003, pp 17–18

31 Ev 55

32 For fingerprint and iris large-scale matching is assumed, whereas for face one-to-one verification is assumed.

33 According to the Home Office, this is equivalent to a false match rate of 0.000000013% and a false non-match rate of 1%.

34 According to the Home Office, this is equivalent to a false match rate of 0.0000000005%.

BIOMETRIC TECHNOLOGY OVERVIEW

Fingerprinting

The use of fingerprinting is well-known because of its use in forensic science and law enforcement. Large-scale fingerprint technology works by using coordinates of points on the fingerprint where ridges end or split. It is also possible to match the whole fingerprint pattern but such systems are rarely used on a large scale.

There are two main ways of recording fingerprints: rolling and slapping. Rolled fingerprints are used in law enforcement where the maximum print is recorded. Slapped fingerprints only record the pad of the finger but the process is less intrusive. There are different types of fingerprint reader: slap readers (10 prints), single-finger optical readers, single-finger capacitive readers, ultrasound readers and rolled fingerprint readers. It is likely that the ID Cards Programme would use a 10-finger slap reader.

The basic characteristics of fingerprints do not change, although fingerprints can be damaged by injury, burns or wear due to work. When recording fingerprints, it is important the finger is clean because any grease or dirt can distort the image. The image can also be distorted by pressure on the finger that alters the fingerprint pattern.

There are hundreds of fingerprint companies but only four or five provide AFIS (automated finger identification systems). There are several large-scale fingerprint databases including the FBI AFIS database, which has a database of 47 million fingerprints and Ident1 in the UK, which holds six million sets of prints.

Facial Recognition

Facial recognition works by identifying people according to sections of the face least susceptible to alteration eg. upper outline of eye, sides of mouth, cheekbones.

The two main methods are: local feature analysis and the Eigenface method. Local feature analysis measures the relative distances between landmarks on the face. The Eigenface method looks at the face as a whole and uses combinations of 2D templates that represent distinctive characteristics of a facial image.

Face recognition readers vary greatly in technology and the lighting of the face can have a great effect upon the performance of the technology. There are approximately 10 companies offering 3D technology and less than 100 companies offering 2D solutions.

Iris Scanning

Iris recognition measures the iris pattern in the coloured part of the eye. Iris patterns are formed randomly at birth and iris patterns are different for every eye. The iris can have more than 250 distinct features compared with 40 or 50 comparison points for fingerprints.

Iris scanning involves a camera capturing an image of one or both eyes. The camera focuses on the eye, locates the iris and accounts for areas obstructed by eyelashes or eyelids. This image is broken into circular grids and each area is analysed for unique patterns. This information is converted into an algorithm in the camera that can be used as a template.

Iris patterns are unique, even between identical twins, and these patterns are stable throughout life. There can be some difficulties with iris scanning if individuals are wearing glasses or contact lenses, if they have aniridia (lack an iris) or glaucoma.

The iris recognition market is currently dominated by Iridian, although it may become increasingly competitive as patents expire. Iris performance statistics from independent tests are limited to 100's. However, the technology is widely used in the United Arab Emirates, which has a database of over 350,000 iris scans.

Source: Government Memorandum, Appendix 2, Ev 54-67.

19. One of the risks of biometric technologies is that they might be spoofed, which means that real biometrics are replaced with false ones. Spoofing is usually attempted by re-activating a latent image from a previous enrolment; using a false biometric for example contact lenses, or using a biometric from another individual, alive or dead. Technology is currently being developed that would be able to distinguish live biometrics. The

Government memorandum emphasises that in order to spoof the system it will also be necessary to conceal attempts from the trained operator.[35]

20. Biometric technology is becoming increasingly popular as part of identity and passport schemes. In the last five years, there has been a rise in the use of biometrics on visas and passports:

- Following 9/11, the United States introduced fingerprint biometric visas for those visiting the US. We observed this scheme, the US-Visit programme, at JFK airport in New York during our visit in March 2006.[36]
- In May 2003, the International Civil Aviation Organization (ICAO) adopted a blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs).[37]
- In June 2003, a border control programme based on iris scanning was rolled out throughout the United Arab Emirates.[38]
- In December 2004, following European Parliamentary approval, a new Regulation on passports in the Schengen States was adopted by the Council of Ministers. It provided that newly-issued passports must include digital facial images (within 18 months) and fingerprints (within three years).[39]

It must be noted however that none of these schemes are as ambitious in their use of biometrics as the UK identity card scheme, which will be the first national scheme to use three biometrics.

Information and communication technology

21. The ICT system that will be a central part of the identity cards scheme will consist of one logical database (the National Identity Register) and smart cards. The Home Office has stated in written evidence that the system will be split into modules that will be met wherever possible by customised versions of systems already found in the marketplace. This solution will be used as a reference point for the eventual system design undertaken by the suppliers. The Home Office states that "this modularisation is intended to simplify, and hence help de-risk, IT system delivery, and allow easier substitution of any modules that fail to meet our capability, performance and resilience requirements".[40] It also claims that modularisation will highlight security violations because the information flowing between systems will be visible and auditable.

22. In oral evidence to the Committee, Katherine Courtney emphasised that the National Identity Register was not necessarily going to be a central database. She explained that "The

35 Ev 60

36 Philip Shenon, "U.S. high-tech screening for foreigners", *The International Herald Tribune,* 1 May 2003, p 2.

37 www.icao.int/mrtd/biometrics/recommendation.cfm

38 www.iridiantech.com

39 Council Regulation (EC) No.2252/2004

40 Ev 73

National Identity Register will be a technical system that may involve a series of data storage solutions".[41] The identity cards programme team is focusing upon the outputs of the system and as a result the National Identity Register could be a single monolithic database or a series of databases. Until procurement begins, there is little more information available regarding the likely technology that will be chosen (see paragraph 125).

23. The identity cards will use smart card technology. Physically, the card will be a piece of plastic, like a credit card, with an embedded chip that will contain biographical and biometric data. It will show the individual's name and an image of their face. Each card will have its own Identity Registration Number (IRN) and a Personal Identification Number (PIN), which can be set by the cardholder. Cards can either use contact technology requiring physical connection with a reader or contactless technology like that which is currently used in Transport for London Oyster cards. The identity cards scheme is expected to use a card that could function both as a contact and contactless card. On 20 July 2005, the then Parliamentary Under-Secretary of State for Immigration, Citizenship and Nationality, Andy Burnham stated that:

> "It is currently planned that identity cards issued to British nationals eligible for a passport could be used by individuals for travel within Europe. In order to facilitate this, the card will need to meet standards established by the International Civil Aviation Organisation (ICAO), which require the card to be contactless in order to be considered a valid travel document. In addition, we are also investigating whether it would be beneficial and cost effective to be compatible with other card reader national infrastructures, such as the Chip & PIN network, which requires contact card. Thus it is possible that an identity card will function as both a contact and contactless card."[42]

The Home Office has not yet publicly finalised these plans.

41 Q 346

42 HC Deb, 20 July 2005, col 1783W

3 Stakeholder engagement

24. The development of the identity cards scheme involves a large number of different organisations and groups including Government departments, Local Government, academic experts, industrialists, and officials from similar schemes in other countries. As will be explored in the following chapter, each of these groups represents a valuable source of scientific advice that the Home Office could be exploiting. Before dealing with each group in detail however, we will consider several over-arching issues in relation to stakeholder engagement that have been highlighted during our inquiry.

Consultations

25. The Home Office has undertaken two main consultations; the first regarding the notion of an entitlement card in general and the second focusing on the legislation on identity cards. The first consultation on entitlement cards and identity fraud ran from July 2002 until January 2003.[43] It concentrated upon the purpose of the card, how cards might be issued, what information would be stored on any register and the cost of the scheme. The second consultation on the legislation on identity cards included some reference to the technology that might be used such as a National Identity Register, cards and biometrics.[44] It also covered several other areas dealt with by the legislation, such as regulations, data-sharing powers, compulsion and the information that would be recorded. This consultation ran from April 2004 until July 2004 and involved contacting stakeholders, using focus groups, undertaking quantitative surveys and giving presentations.[45]

26. More recently, the Home Office has run market-sounding exercises with industry, hosted by Intellect, that have focused on specific areas of requirements in technology. For instance, 35 companies participated in the verification systems seminar and 51 companies took part in the security systems seminar.[46] The Home Office has also sent specific questions to selected companies to provide detailed information on market capability. The Home Office explained that "Our contact with industry has been to share the high-level intentions of the Identity cards programme with companies and invite their reaction and feedback, and also to question them on specific technical areas".[47]

27. The Home Office believes that it has consulted widely on the identity cards programme. In oral evidence to us, Katherine Courtney said that "we have been consulting with industry about our plans…I do not think that we have in any way run the risk of not being open enough with industry. I think we have applied best practice in this area".[48] Professor Paul Wiles, the Chief Scientific Adviser at the Home Office has stressed the importance of consultation, stating that "it is extremely important that we regularly test the

43 Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper,* Cm 5577, July 2002

44 Home Office, *Legislation on Identity Cards—A Consultation,* Cm 6178, April 2004

45 Home Office, *Identity Cards: A Summary of Findings from the Consultation on the Legislation on Identity Cards,* Cm 6358, October 2004

46 Ev 114-115

47 Ev 114

48 Q 338

assumptions that we are operating on and our perceptions against a wider public understanding".[49] In general, relevant organisations have acknowledged that the Home Office has attempted to consult them regarding the identity cards programme. Intellect has said it "welcomes the basic approach taken by the Home Office during its period of consultation and deliberation".[50]

28. The evidence that we have received however suggests that there have also been several problems with the consultations. First, the nature and regularity of meetings does not seem to have satisfied the community. In written evidence to us, Peter Tomlinson from Iosis Associates stated, "That there were meetings at which HO [Home Office] was present and independent experts were also present is not disputed, but these were not HO consultations".[51] We also heard in oral evidence from Nick Kalisperas, Director of Markets at Intellect, who said that "there is a difference between consulting widely and having regular consultation".[52] In the same evidence session, Dr Tony Mansfield from the National Physical Laboratory noted that he thought that there could have been "better engagement between the original consultation and procurement, and there were perhaps a few opportunities that were missed for engagement with industry and academia to investigate certain solutions or certain problems prior to the procurement starting".[53]

29. Secondly, the evidence raised concerns that the consultations did not ask the right questions at the right time. Professor Thomas from the UK Computing Research Committee (UKCRC) said that "the consultation did not start at the right level", whilst Dave Birch from Consult Hyperion explained that "if you are consulting industry about whether the card should be red or green, that is very different from consulting industry about whether there should be a card" or another identity management solution that does not use cards.[54] The consultation process seems to have left the community with a lack of confidence regarding the scheme. Jerry Fishenden from Microsoft said that "after all these consultations we still do not seem to have had an impact on the level of understanding about what makes for a good identity system to practise".[55]

30. It was also frequently commented that the consultations appear to have focused unduly upon procurement issues. In written evidence, Microsoft said that "the current phase of public consultation by the Home Office has primarily focused on issues of procurement".[56] Jerry Fishenden from Microsoft elaborated that "every time we came close to wanting to talk about the architecture, we were told that was not really up for discussion because there was an internal reference model that the Home Office team had developed themselves, and that they did not feel they wanted to discuss their views of architecture".[57] Dave Birch agreed, saying that "A lot of the consultations tend to be discussions about the structuring

49 Q 1127, HC 900-x, (to be published in HC 900–II, Session 2005–06)

50 Ev 103

51 Ev 99

52 Q 471

53 Q 522

54 Q 475 (Thomas), Q473 (Birch)

55 Q 489

56 Ev 127

57 Q 476

of procurement and how exactly the procurement would work, and not really the kind of consultation that you would expect at a more scientific level, consultation about how the scheme should work overall and what it should do".[58]

31. **The Home Office has consulted the wider community and has tried to apply best practice in this area. However, stakeholders are not satisfied with the nature of consultation and feel that consultations have been unduly limited in scope with unclear evidence gathering objectives. As a result, the wider community does not have the level of confidence in the scheme that could be expected following a successful consultation process.**

32. The Home Office may be reluctant to allow wide-ranging discussion of technical matters because it is concerned that this may jeopardise the procurement process by suggesting to the market that particular solutions are favoured. The Home Office noted that if the market believed that a particular solution was being sought, it would be "losing the advantages of setting output-based requirements—that is, promoting innovation in the supplier community and allowing suppliers the ability to use their specialist expertise unhindered by being steered down a narrow technical path".[59]

33. Given that the identity cards scheme is still in the pre-procurement stage, it is possible for the Home Office to adopt a different approach. We have received several suggestions about the ways in which the Home Office could engage successfully with its stakeholders in the coming months. Microsoft has proposed that the "next stage should adopt the approach taken by the US State Department, which created a model that actively encourages broad, open dialogue in pursuit of improved outcomes".[60] Furthermore, it asserts that "correctly constructed, such consultation need have no implications for any 'pollution' (real or perceived) of subsequent procurement processes".[61] Nick Kalisperas from Intellect has similarly said that "as we approach procurement, there should be more intensive consultation specifically with the industry, so that the industry has a full and clear picture from which they can decide whether to bid for this programme or not".[62] The Home Office should consider how it might change its approach to stakeholder engagement. We acknowledge that the Home Office may be concerned about discussing technical issues because it believes that this may jeopardise the procurement process. However, we believe that innovative solutions are more likely to be stimulated by open debate with a well-informed, engaged community than limited discussion with a confused community. **We recommend that the Home Office undertakes future consultations on scientific and technical issues as well as the procurement process.**

Transparency

34. Several submissions that we received highlighted the lack of transparency in the identity cards programme, particularly in relation to the processes by which advice feeds

58 Q 473

59 Ev 124

60 Ev 126

61 Ev 127

62 Q 471

into policy. The Local Authority Smartcard Standards e-Organisation (LASSeO) has said that "Like other players outside central Government, we find the whole process highly opaque".[63] The British Computer Society (BCS) focused in particular upon the lack of feedback once scientific advice had been given about how this input had influenced the final policy. It states that "once advice has been offered there is a lack of feedback or follow through process".[64] Furthermore, the BCS commented that "where such advice actually informs policy those involved should be acknowledged and communicated with to ensure full understanding of the advice given".[65] This concern was shared by the Institute of Electrical Engineers (IEE).[66] The IEE observed that "it is generally felt there is very little in terms of published analysis or feedback".[67] It further commented that "There may be some value if future summary documents included information on the response to certain evidence, what was accepted/rejected, or how proposals have been amended".[68]

35. The identity cards programme team has said in future it would be clear and transparent how scientific advice had influenced the technology specifications to be released during procurement. Katherine Courtney said that "we have told industry that we will be publishing our changed thinking as a result of the dialogue we have been having with them and making that publicly available to the industry and we will be doing that".[69]

36. **We conclude that the processes by which scientific advice is incorporated into policy are not completely transparent and that organisations are not receiving feedback regarding their advice. We urge the Home Office to fulfil their welcome commitment to make it clear how and what advice has been incorporated into the development of future policy, particularly the technical specification.**

Clarity

37. The scheme aspirations were set out in the bill and are now outlined at the start of the Identity Cards Act 2006 (see paragraph 8). As detailed earlier, the scheme is intended to prevent or detect crime; to ensure national security; to enforce immigration controls; to secure the efficient and effective provision of public services, and to enforce prohibitions on unauthorised working or employment.[70] The emphasis placed on different aspirations has varied throughout the life of the scheme and this changing focus has resulted in a lack of clarity regarding the likely technology requirements. For example, whereas originally the focus was on tackling identity fraud, it soon changed to countering terrorism and combating crime.[71] In oral evidence when asked about the objectives of the scheme, Joan Ryan, the Parliamentary Under-Secretary of State for nationality, citizenship and

63 Ev 93

64 Ev 82

65 As above

66 This organisation is now known as the Institution of Engineering and Technology (IET).

67 Ev 77

68 Ev 78

69 Q 339

70 *Identity Cards Act 2006,* para 1(3–4)

71 See speeches by David Blunkett: HC Deb, 11November 2003, col 171 & HC Deb, 19 July 2004, col 23

immigration acknowledged that "It is true that people have sometimes given them in a different order and perhaps with a different emphasis".[72] **We are aware that political pressures inevitably impact on the scheme, but it is highly regrettable that the emphasis on different aspirations has changed. This has created uncertainty for the public and industry alike. We hope that the situation will stabilise now that the Bill has received Royal Assent.**

38. Although the scheme aspirations are now clearly laid down, there is still a lack of information regarding how these aspirations will be delivered by the scheme. Jerry Fishenden from Microsoft has called this lack of a clear link between aspiration and practical detail the missing "technology policy" layer.[73] Professor Martyn Thomas from the UKCRC stated that "everything…that I have seen about the programme, lays down a set of aspirations for the ways in which the identity scheme might contribute to reducing fraud under some circumstances, but there is no quantification, there is no analysis".[74] This missing information includes a lack of detail regarding the scope of the scheme, the involvement of different Government departments and the ways in which individuals will actually use their identity cards. The Government needs to clarify the details of the scheme in order to successfully develop the technical architecture that is required to support it. Microsoft stated in written evidence that "the overall technical architecture…is clearly inter-dependent on the policy and business requirements and objectives of the ID card scheme".[75] Professor Thomas from the UKCRC agreed, saying in oral evidence that "It is clear that the technology is interdependent with the business case because the business case is founded on the requirements and the technology should be there to support the requirements".[76]

39. It is unsatisfactory that the boundaries of the scheme still seem not to have been set. We have the impression that the Government still does not know precisely what it wants from the identity card scheme. In October 2005 for example, the Home Office estimated that the number of verification transactions would be 163 million per annum. In May 2006 the Home Office's estimate of the number of verification, identification, authentication and information provision services had risen to 771million per annum. The Home Office said that the rise resulted from "the progress made in understanding public and private sector organisations' intended use of the scheme".[77] The Home Office asserts that it intends to ensure that a solution can be scaled up to the demand required rather than developing the scheme around a number of fixed transactions.[78] However, this assertion implies that the Home Office is not confident either in its estimates regarding the number of transactions or in its awareness of the intended uses of the scheme by public and private organisations.

40. There is also apparent confusion regarding the use of the identity card across Government. In oral evidence to us, the Parliamentary Under-Secretary of State for

72 Q 1143

73 Jerry Fishenden, *Weblog*, 31 October 2005. http://ntouk.com/archives/2005/Oct/31.10.2005.htm

74 Q 492

75 Ev 127

76 Q 492

77 Ev 112

78 As above

nationality, citizenship and immigration, Joan Ryan, said that the Home Office was in discussions with the Department for Work and Pensions, the Department of Health, the Criminal Records Bureau, the police and the Department for Communities and Local Government. She explained that "we are attempting to get this cross-departmental recognition of benefits, the buy-in and working together".[79] There still appears to be confusion regarding whether the NHS will use the card. In October 2006, the then Home Secretary, Rt Hon Charles Clarke MP, said that "no medical details will be on the database".[80] In April 2006, the then Parliamentary Under-Secretary of State for Immigration, Citizenship and Nationality, Andy Burnham MP said that "you could argue that blood group, allergies, donor status, that sort of information could be potentially helpful" and he proposed that this information could be placed voluntarily on the National Identity Register.[81] However, soon afterwards in response to an article published on 15 April 2006 in *The Independent,* the Home Secretary Charles Clarke wrote that the National Identity Register would not include health or medical records.[82] This issue was raised by Dr Edgar Whitley from the London School of Economics in an oral evidence session.[83] More recently, there has been disagreement regarding the release of information concerning the likely uses of identity cards by the Department for Work and Pensions (DWP). In December 2004, an FoI request was made to the DWP for a copy of the Department's feasibility study on identity cards. The DWP refused this request and on 11 July 2005 the individual asked the Information Commissioner to make a decision about the handling of the request.[84] On 5 June 2006, the Information Commissioner, Richard Thomas, decided that the information was in the public interest and should be released. He said that "there is clearly a strong public interest in the public knowing whether the introduction of identity cards will bring benefits to the DWP, and to other departments, and if so what those benefits will be".[85] This lack of transparency and reticence to share information regarding the cross-departmental uses of the scheme damages public confidence. It also adds to the impression that the Government has not yet determined the scope of the scheme. It seems that the Home Office is willing to expand the scheme at a later date. On 14 June 2006, Joan Ryan MP said that the main aspirations of the scheme "should not exclude developmental work on using the card in other ways as time moves on".[86]

41. As already noted, the Home Office is taking an incremental approach to the identity cards scheme (paragraph 10). The Home Office has, however, not clarified what the various incremental steps towards identity cards will be beyond the introduction of biometric passports. On several occasions, the Home Office has referred to different schemes as precursors to identity cards and this has resulted in a lack of clarity between the introduction of identity cards and other registration documents, which use biometrics. In

79 Q 1184

80 Isabel Oakeshott, "Labour U-turn over ID card medical details", *The Sunday Times,* 23 April 2006, p 13.

81 As above

82 http://press.homeoffice.gov.uk/Speeches

83 Q 536

84 Information Commissioner's Office, *Decision Notice: Department for Work and Pensions,* 5 June 2006

85 "Whitehall fights ID costs demand", *BBC News Online,* 5 July 2006, http://news.bbc.co.uk/1/hi/uk_politics/5150584.stm

86 Q 1149

oral evidence, the Minister Joan Ryan stated that "I was watching ID cards being issued yesterday at Lunar House in Croydon. The ARC [Application Registration Card] card for asylum seekers is, in effect, an ID card".[87] Application Registration Cards were launched in February 2002.[88] The cards contain two digital images of the holder and the holder's fingerprint details.[89] The Home Office has also said that the identity cards programme would begin with the introduction of "biometric residence permits for foreign nationals in 2008".[90] It is unclear whether full identity cards, including the three proposed biometrics, will also be introduced in 2008. Indeed there have been reports of an "early variant" identity card that would include a facial image or two fingerprints (see paragraph 10). The Home Office has not clarified the situation by saying that there are no "firm plans" for a different type of card to be issued earlier than others.[91]

42. We are surprised that the scope of the scheme has still not been finalised. There is insufficient evidence to suggest that uses across Government have been explored fully. As will be discussed in more detail in the following chapter, interoperability is crucial to the success of the scheme and the longer that the Government takes to determine its scope the more difficult it is likely to become to make sure that the technology is interoperable. **We urge the Home Office to finalise the scope of the scheme and the technical standards needed for interoperability as soon as possible.**

43. This lack of clarity regarding the overall scope of the scheme is exacerbated by a lack of detail concerning when, where and how identity cards might be used. The Home Office website currently contains three examples of how an identity card might be used in daily life to prove your age, collect a parcel or transfer money.[92] This lack of detailed information regarding precise scenarios has been highlighted in written and oral evidence. LASSeO has stated in written evidence that, "It is very difficult to establish what detailed plans exist or are being developed, what technologies will be selected, how these technologies will be used, etc.".[93] Jerry Fishenden from Microsoft explained that "I would have expected at this stage to see a fairly rich set of very precise scenarios about exactly where and how the ID card would be used and to address many of the issues we are talking about here as to what gets released in those types of scenario".[94] He also noted that "I have heard nothing in any of the consultation about how this card would operate in an online context".[95] Furthermore, he has questioned whether, if a chip and pin type of technology is going to be used in the majority of scenarios, the debate on biometrics has been "a bit of a side issue".[96]

44. Representatives from the UKCRC and Microsoft have also highlighted the lack of clarity regarding when the identity card would be used for authentication, that is finding

87 Ev 36

88 "Application Registration Cards for Asylum Seekers launched", 1 February 2002, www.refugeecouncil.org.uk/news

89 Home Office, *Application Registration Card (ARC) and Standard Acknowledgement Letter (SAL),* July 2006

90 Ev 129

91 Ev 128

92 www.identitycards.gov.uk/how-idcard-daily.asp

93 Ev 95

94 Q 493

95 Q 502

96 As above

out if you are eligible to do something, and identification, which is finding out who you are.[97] Professor Martyn Thomas from UKCRC explained that "If you go that extra step to ask for identity information when what you actually want is authentication…you are revealing information which makes things like identity fraud much more likely to occur".[98] Jerry Fishenden from Microsoft referred to two examples on the Identity and Passport Service website, which described that an identity card would be used to reveal an individual's date of birth so that they could buy alcohol at 18 or get a pensioner's discount at 65. He questioned "Why would you want to reveal somebody's date of birth in that scenario?...You do not even have to reveal their age, but that they are over 65".[99]

45. **In order to clarify when and how the card might be used, we recommend that the Home Office releases more information regarding what personal data will be revealed in different scenarios, including in an online context. Until this information is released, it is difficult to ascertain the true scope of the scheme and to fully understand how technology will be used within the scheme.**

46. The evidence that we have received has also highlighted a lack of clarity in another area of the identity cards programme: the procurement process. In general, industry appears to be unsure about when the specifications will be released and, when they are released, what they are likely to be.[100] Initially the procurement process was due to start as soon as Royal Assent had been granted; however several months have passed and the process has not yet commenced. Nigel Seed, Director of the National Identity Register, told us on 22 March 2006 that:

> "We have what we are calling level one requirements which describe not in very detailed terms what we want the programme to do. That will go out initially to all the companies that have expressed an interest. They will come back and tell us what their proposals are. We will then down-select to a smaller group that will receive the more detailed requirements."[101]

However, Intellect has said that they "would like to see a final Statement of Requirements prior to commencement of procurement".[102] We understand that the Home Office is attempting to implement best practice in procurement but we believe that there is a disagreement between Government and industry regarding what best practice actually means. This disconnect may be due to the use by the Home Office of EU terminology regarding procurement. In January 2006, new regulations regarding public procurement came into force in the UK.[103] These regulations use the term 'procurement' to describe what has traditionally been known as the acquisition process. Procurement, ie. the buying stage, was part of this acquisition process, which also involved feasibility, trialling and

97 Q 489

98 Q 489 (Thomas)

99 Q 489 (Fishenden)

100 Andrew Murray-Watson, "ID card scheme start delayed by Home Office", *The Daily Telegraph*, 11 June 2006, p 2

101 Q 273

102 Ev 104

103 Public Contracts Regulations 2006 (SI 2006/5); Office of Government Commerce, *EU Procurement Guidance,* January 2006

piloting. Within the terminology of these new regulations procurement includes a dialogue with suppliers, specification, selection and award. Thus whilst Intellect is seeking a final statement of requirements before procurement begins, for the Home Office discussion about such a statement is part of the procurement process. **We recommend that the Home Office issues a clear timetable for the publication of the technical specifications and defines procurement processes and stages.**

47. The evidence has highlighted four main areas where the Home Office still needs to clarify the scheme: its overall scope, the involvement of other Government departments, the practical uses of the card and the procurement process. These areas were all highlighted in 2004 by the House of Commons Home Affairs Committee's Report on identity cards.[104] In response to this Report, the Home Office noted that "Work is continuing with stakeholders" on the scope of the scheme.[105] In relation to the use of the identity card by other departments, the Home Office stated that "The Government recognises the need for ongoing work on these issues".[106] **We are disappointed that two years after the Home Affairs Committee inquiry into identity cards the problems regarding clarity have not been resolved. We urge the Home Office to address these issues immediately.**

104 HC (2003–04) 130–I, paras 71, 119, 125, 216.

105 Home Office, *The Government Reply to the Fourth Report from the Home Affairs Committee,* Session 2003–04, Cm 6359, October 2002, p 8.

106 As above, p 15.

4 Sources of scientific advice

48. The identity cards scheme relies on several different sources of scientific and technological advice on both the biometric and ICT aspects of the scheme. The Home Office has formalised this advice to a certain extent in relation to biometrics by creating advisory committees. Currently advice regarding ICT is seemingly provided on a more *ad hoc* basis.

Advisory committees

Biometrics

49. The Home Office has set up two advisory committees on biometrics: the Biometrics Experts Group and the Biometrics Assurance Group. The Biometrics Experts Group has gradually evolved during the life of the identity cards programme. The Biometrics Assurance Group first met on 24 November 2005 and again on 20 February 2006 and 15 May 2006.[107] As well as creating these committees the Home Office has sought to enhance its work in biometrics by establishing a Home Office Biometrics Centre of Expertise.[108] This Centre, which opened in November 2005, is based at the Home Office Scientific Development Branch and it is headed by Marek Rejman-Greene.

50. According to the Government evidence, the Biometrics Experts Group "is a group of Home Office and external experts which meets approximately once a month. Its role is to actively contribute to the biometrics requirements of the programme".[109] In oral evidence, Katherine Courtney explained that this meant that the identity cards programme team used the Biometrics Experts Group "in reviewing our own plans, our own understanding, of what the technical risks are and how we can work with the technologies, and also to do that horizon scanning around what is likely to be developing over time".[110]

51. The Biometrics Assurance Group is made up of experts from academia and industry. It has ten members and is chaired by the Government's Chief Scientific Adviser, Sir David King.[111] Its functions include ensuring that the programme's requirements for biometrics are adequately specified, evaluating solutions proposed by suppliers, interpreting the outcomes of testing, and reviewing advice from the Biometrics Experts Group. However, the Assurance Group has only recently begun its work. Dr John Daugman, a member of the Biometrics Assurance Group, said in oral evidence on 3 May 2006 that the two meetings to date had been "mainly briefing opportunities for us to be briefed by Home Office officials and affiliated scientists", although he also acknowledged that "things are accelerating a bit more now".[112]

107 Ev 72

108 Home Office, *Science and Innovation Strategy 2005–08,* November 2005, p 14

109 Ev 72

110 Q 279

111 Ev 73

112 Q 529

52. It is likely that in the future the work of the Biometrics Assurance Group could extend beyond the identity cards programme. In oral evidence to the Committee, Marek Rejman-Greene said that the Biometrics Assurance Group "will also look in the future at all the other related programmes using biometrics, such as the UK Visas Programme, programmes to do with immigration and eBorders".[113] This assertion was supported by the explanation from the Home Office Chief Scientific Adviser, Professor Wiles, regarding the involvement of Sir David King. Professor Wiles said that:

> "This is a new technology which I think is probably going to have wider application. It therefore seemed to me it would make more sense to have an advisory committee that was chaired by the Government's Chief Scientific Adviser so that it could act as a scientific advisory committee in the first instance for the Home Office development but then subsequently for development anywhere else in government."[114]

We note that the Home Affairs Committee recommended in its Report on identity cards that the Government's Chief Scientific Adviser be involved in overseeing biometric testing.[115] This recommendation was accepted by the Government in October 2004 in its response to the Home Affairs Committee Report.[116] It is disappointing that, after accepting the recommendation, the Government took over a year to set up the Biometrics Assurance Group.

53. **We welcome the establishment of the Biometrics Experts Group and the Biometrics Assurance Group, although we regret the time that the Home Office has taken to set them up. We support the involvement of Sir David King and believe that the Assurance Group has the potential to work well, particularly in providing consistent advice across Government. We seek confirmation from the Home Office that the Biometrics Assurance Group will be given the direction, tools and time to fulfil its tasks in practice and that the Group's recommendations will be taken into account.**

Information and communication technology

54. The Government's written evidence asserts that assurance on ICT within the identity cards programme is provided firstly by the Independent Assurance panel made up of representatives drawn from industry and secondly by external review by the Home Office Science and Technology Reference Group. The Independent Assurance panel consists of four members with experience of large-scale projects in the public and private sector. The Home Office explained that the panel "provides oversight of the programme's ability to deliver the scheme".[117] The panel not only provides assurance on ICT but also on marketing, organisational change, risk and fraud. The Science and Technology Reference Group covers all science and technology within the Home Office and is chaired by the Permanent Secretary. The membership is drawn from the learned societies and in

113 Q 283

114 Q 1128, HC 900–x, (to be published in HC 900–II, Session 2005–06)

115 HC (2003–04)130–I, para 39

116 Home Office, *The Government Reply to the Fourth Report from the Home Affairs Committee,* Session 2003–04, Cm 6359, October 2002, p 21

117 Ev 117

November 2005 the Committee had eleven members, including the Permanent Secretary and departmental Chief Scientific Advisor.[118] Only one of these members, Dr Michael Rodd, specialises in computing.

55. We acknowledge the roles played by the Independent Assurance panel and the Science and Technology Reference group in providing assurance on ICT. However, we are concerned that although these panels have important roles in addressing generic issues, they may not be best-placed to offer expert advice regarding ICT. We welcome the balance of in-house and external advice regarding biometrics and recommend that a similar approach is used for ICT. We also note that the input of external experts has been recently formalised by another department, the Department of Health, in its Connecting for Health Programme. The role of advisory committees more generally will be explored in the over-arching report into scientific advice, risk and evidence. **We recommend that the Identity and Passport Service establish an ICT Assurance Committee consisting of academics and industry experts and that this committee reviews the programme specifications relating to ICT.**

56. Furthermore, we note that references regarding who has responsibility for ICT in the identity cards programme have been noticeably absent from the Government's evidence. Professor Wiles told us that "I do not have responsibility for ICT in the Department".[119] We were told informally by the Science Secretariat at the Home Office that the Chief Information Officer, Vincent Geake, had responsibility for ICT advice within the Home Office, including the identity cards programme. However, this was later qualified in a written response by the Home Office that stated "Vincent Geake is responsible for providing advice about ICT strategy, but not about ICT delivery within programmes".[120] The Home Office noted that the principal way that the Chief Information Officer was engaged with the identity card programme was through meetings of the Programme Board.[121] The response provided little further detail regarding the possible sources of ICT advice within the identity cards programme and did not explain the role of the Chief Information Officer within the Identity and Passport Service (see Figure 1, page 10).

57. Since 2004, as part of its Transformational Government agenda, the Government has developed the roles of Chief Information Officers and Chief Technology Officers.[122] The Chief Information Officer and Chief Technology Officer should in principle be part of a joined up, Government-wide ICT profession that is aiming to improve performance of Government ICT resources and helping to find solutions to common problems using technology.[123] However, there appear to be problems with the implementation of this strategy within the Home Office and in relation to the identity cards programme in particular. First, we have not seen any evidence to suggest that the Home Office has a Chief Technology Officer. Secondly, the roles of the Home Office Chief Information Officer and the Identity and Passport Service Chief Information Officer are unclear in relation to the

118 Home Office, *Science and Innovation Strategy 2005–8,* November 2005, p 36

119 Q 1131, HC 900–x, (to be published in HC 900–II, Session 2005–06)

120 Ev 122

121 As above

122 Cabinet Office, *Transformational Government Enabled by Technology* , Cm6683, November 2005, p 16

123 www.cio.gov.uk

identity cards programme. Although we were assured in relation to scientific and technological advice that "the mechanisms to be used by Identity and Passport Service will not be substantially different from those used prior to the formation of IPS", it seems that the establishment of the agency has caused confusion and in ICT in particular, responsibility for advice is unclear.[124] **We welcome the work that has been undertaken over the last two years by the Government in developing the network of Chief Information Officers and more recently, Chief Technology Officers. We have not received any evidence demonstrating that these changes have impacted upon the identity cards programme. Given the central role played by ICT in the identity cards programme, we recommend that the involvement of ICT professionals within Government in the scheme be made clear and, if appropriate, that the Chief Information Officer chair the ICT Assurance Committee.**

Academia and learned societies

58. Although the Home Office has engaged productively with representatives from academia in some aspects of the programme, such as the Biometrics Assurance Group, in other areas evidence has shown that a dialogue about scientific advice with academics has been less visible and successful.

UK computing community

59. The UK Computing Research Committee (UKCRC) was highly critical of the Home Office's approach to the academic computing community. In oral evidence, Professor Martyn Thomas of the UKCRC said that, "I do not think there has really been any consultation with the academic community".[125] It seems however that the academic community is keen to offer advice on ICT. The evidence submitted to us by the UKCRC catalogues a series of attempts to engage with Government officials regarding ICT issues with little apparent success. This written evidence concludes that "overall, we have been disappointed with the extent to which scientific evidence has been sought or used in our area of expertise".[126] The involvement of the academic community is important because, as Professor Thomas pointed out, it is "independent and therefore can bring something to a consultative process that industry really cannot because we can stand back as independent academics and look at the viability of something and look at best practice without having a vested interest of any sort".[127]

60. Despite its apparent lack of direct contact with the academic ICT community, the Home Office is still reliant upon its advice. In oral evidence to the Committee, Nigel Seed Director of the National Identity Register explained that "The British Computer Society put out quite a comprehensive report on the complexity of IT projects…They listed the ten most common causes of failure…I went through this and we have ticked the box and we have learnt from the Computer Society who are the experts in the field".[128] In response to

124 Ev 118

125 Q 475

126 Ev 75

127 Q 475

128 Q 333

written questions from us, the Home Office also noted that its decision to use a modular IT architecture was supported by same report.[129]

61. We are perplexed as to why the identity cards programme team does not approach the ICT academic community directly rather than merely using published material. **We believe that the Home Office is not taking full advantage of the impartial advice that could be offered by the academic computer science and information systems community. We recommend that the Home Office uses the ICT Assurance Committee in order to fully engage the academic ICT community.**

London School of Economics Identity Project

62. The London School of Economics (LSE) has featured strongly in the debate on identity cards because it has published several reports considering the Government's proposals. The written evidence submitted by the LSE notes that the Department of Information Systems at LSE began research into authentication and identification systems in the 1990s. In 2003 this progressed to research to inform policy and the public debate on identity cards. This research culminated in several reports: the Interim Report in March 2005, the Identity Project Report in June 2005 and the Research Status Report in January 2006.[130]

63. The LSE Identity Project Report was critical of the identity cards scheme and proposed an alternative scheme. According to the LSE, its reports have "questioned some of the key policy goals of the ID cards scheme, reviewed the likely effects on policing, assessed the challenges and risks in the Government's proposals, and offered an alternative scheme for public consideration".[131] The LSE reports have attracted a lot of publicity and although the reports considered various aspects of the scheme, debate has focused on the costs of the scheme. The assertions made by the LSE and the Government regarding costs will be dealt with in more detail in the following chapter (see paragraph 100).

64. It seems that the LSE reports were intended to stimulate discussion regarding the Government's proposals. In oral evidence to the Committee, Professor Angela Sasse, Professor of Human-Centred Technology at University College London explained that "the intention was to seek a constructive debate"[132] Unfortunately, the reports created a debate that appeared at times to be more destructive than constructive. Dr John Daugman from Cambridge University has noted that "public debate about the proposed biometric ID cards has been dominated by a single document, the 'LSE Report'".[133]

65. Given the central role that the LSE reports have played in the debate regarding identity cards, it is unfortunate that the information released by the LSE at an early stage had factual errors, particularly in relation to technology. For example, the LSE acknowledges that there were errors in its interim report confusing the iris with the retina. It has written that "in our *interim* report our lack of specialist advice in the area meant that we did

129 Ev 118; Royal Academy of Engineering & British Computer Society, *The Challenges of Complex IT Projects,* April 2004

130 LSE, *The Identity Project: Interim Report,* March 2005; LSE, *The Identity Project: An Assessment of the UK Identity Cards Bill and its implications*, June 2005; LSE, *The Identity Project: Research Status Report,* January 2006

131 Ev 87

132 Q 563

133 Ev 83

confuse the two and we sought specialist advice and made many corrections before issuing our *main* report in June 2005".[134] The Identity Project Report was overseen by a steering group of 14 professors and we note that 79 of the 91 recommendations made by this report supported, or supported conditionally, recommendations made by the Home Affairs Committee in July 2004.[135] **The LSE reports served a useful purpose in opening up debate on the scheme but the resulting emphasis upon the cost of the scheme and the errors in the initial interim report inhibited the development of the necessary wide-ranging debate.**

66. Some of the controversy surrounding the LSE reports has resulted from the Government's reaction to them. The Home Office response to the LSE Identity Project Report outlined the Government's concerns regarding the LSE's cost assumptions and identified apparent weakness in the LSE's alternative scheme and inaccuracies in the report. It did not recognise any benefits within the LSE scheme or acknowledge any of the recommendations. The Home Office asserted that that LSE report was "vague in parts", "contradictory" and contained a "number of inaccurate assumptions".[136] On 18 January 2006, the Prime Minister told the House of Commons that "As for the calculations made by the LSE, I think that I am right that, although the report was put out under the LSE's name, it was actually written by the leading campaigner against ID cards on the ground of civil liberties. So I do not think that it is an entirely objective assessment".[137] According to the submission from the LSE this comment was one of many "spurious, misleading and ad hominem attacks on the reports and its authors".[138] In oral evidence, Professor Angela Sasse said that "I have been quite astonished by the way in which the Home Office reacted against the report because the intention was to seek a constructive debate and unfortunately it did not quite work that way".[139]

67. **We are disappointed by the nature of the Government's reaction to the criticisms outlined in the LSE reports. We believe that the way in which the LSE reports have polarised the debate regarding identity cards, whether intentionally or not, has been detrimental. The Home Office would have been better advised to put together a dispassionate critique of the LSE Identity Project Report rather than seek to undermine its credibility and motivation.**

Industry

68. Industry is a key source of scientific and technological expertise in the areas of ICT and biometrics. Many companies are eager to feed scientific advice into the identity cards programme. Microsoft for example, states that, "The industry has learned many lessons around identity, privacy and security and we are keen to share this knowledge more

134 LSE, *Rebuttal to evidence submitted to Committee by Dr John Daugman*, 28 April 2006, p 4 (www.csrc.lse.ac.uk/idcard/LSE_DaugmanResponse.pdf)

135 Edgar Whitley, "Mistaken Identity", *The Parliamentary Monitor,* June/July 2006, p 32

136 Home Office, *Home Office Response to The London School of Economics' ID Cards Cost Estimates & Alternative Blueprint*, July 2005

137 HC Deb, 18 January 2006, col 833

138 Ev 88

139 Q 563

widely".[140] We recognise that industry has a vested interest the scheme in terms of winning contracts. Companies are keen to provide scientific advice because this could have a beneficial impact during the procurement process. However, it must also be noted that industry wants the scheme to succeed for reputational reasons. Jerry Fishenden from Microsoft explained that "I do not think anyone in industry would like to be here in 2, 3, or 5 years time, whatever the time scale might be, explaining why yet another major public sector IT project has gone off the rails if that were to happen".[141]

69. The Home Office has undertaken market sounding exercises and other forms of consultation with industry. As we have already explained, this process has not produced confidence in the identity cards scheme within the private sector (see paragraph 29). We reiterate our earlier recommendation that the Home Office engages in a wide-ranging debate regarding the scientific and technical aspects of the scheme with industry, to complement the procurement process.

70. We are also concerned that industry representatives may not have taken every opportunity to raise concerns regarding the scheme due to a fear of the commercial consequences. Jerry Fishenden from Microsoft wrote in an article for *The Scotsman* that "When we attend meetings with the Home Office I have noticed that representatives do not voice their concerns very much. Only out of meetings do you hear their concerns".[142] This reticence has perhaps been exacerbated by the lack of clarity regarding the procurement process, which has resulted in industry not knowing if commenting critically would harm their chances (see paragraph 46). It is therefore surprising, given the importance of commercial interests, that some industrial representatives such as Jerry Fishenden from Microsoft have taken the relatively unusual step of publicly criticising the scheme. In these circumstances, the issues that they have raised such as clarity, interoperability and the assessment of risk should be treated as particularly significant. We are also concerned that these individuals have been forced to write articles or give lectures because there are no channels through which they can feed their advice directly into the identity cards programme. **We recommend that, particularly as it enters the procurement phase, the Home Office works to develop further its relationships with industry. Industry is a significant source of scientific and risk reduction advice as well as being a pool of potential suppliers. We reiterate that the Home Office needs to engage in wide-ranging debate with industrial experts regarding scientific and technical aspects of the scheme.**

Co-ordination within Government

71. There is also a wealth of experience in large ICT systems and some biometrics programmes within Government. It is particularly important that this technical expertise and experience is available to the identity cards programme. Furthermore, given that identity cards may be used by several departments, it is crucial that these departments are involved in specifying the technology and ensuring interoperability. In May 2006, a new Ministerial Committee on Identity Management chaired by the Leader of the House of

140 Ev 126

141 Q 483

142 Ken Young, "Microsoft slams UK ID card database", *Vnunet,* 18 October 2005

Commons was created.[143] The Committee includes Ministers representing 16 portfolios: Treasury; Foreign and Commonwealth Affairs; Trade and Industry; Home Affairs; Health; Cabinet Office; Northern Ireland and Wales; Constitutional Affairs; Education and Skills; Communities and Local Government; Work and Pensions; Environment, Food and Rural Affairs; and Transport. This Committee is intended to "co-ordinate the Government's policy and strategy on identity management in the public and private sectors, and to drive forward the delivery of transformational benefits across government".[144] The Committee will be supported by an Identity Strategy Management Group with representatives from key departments at Director-General level.

72. We have received evidence regarding several specific groups that enable cross-departmental working within the identity cards programme. The Home Office explained that an assessment of smart card technologies was aided by expertise from the Department of Transport.[145] The Home Office also has a biometrics practitioners' group, "Goldfinger", which has representatives from the eBorders programme, the FCO and other projects such as the facial recognition testing project.[146] The National Physical Laboratory (NPL) submission notes that it "has seen some evidence that the Home Office is engaging in horizon scanning activities with other government departments".[147] Furthermore, the NPL states that the "cross-departmental government Biometrics Working Group (BWG) [which] has been in existence for some years, provides a mechanism for sharing advice on biometrics across government".[148]

73. The evidence that we have received has highlighted two main areas of concern with regard to co-ordination on this issue within Government. Firstly, there has been a lack of communication between programmes that have a level of technological overlap such as the e-Borders programme or the then Office of the Deputy Prime Minister (ODPM) Smart Card project. The e-Borders programme involves pre-boarding electronic checks of everyone flying to the UK, the collection of information from people on arrival and the monitoring of departures. As part of this programme, Project IRIS (Iris Recognition Immigration System) has been implemented at Heathrow, Gatwick, Birmingham, Manchester and Stansted airports. This system stores and verifies the iris patterns of qualified travellers. Qinetiq has stated that:

> "there appeared to be some duplication in technologies being sought between the NICP [National Identity Card Programme] and eBorders programme. These are two very similar programmes, with similar aims, being run by two different departments [Directorates] within the Home Office with no apparent coherence although it would be fair to recognise that matters have improved over the past nine months."[149]

143 Ev 124

144 www.cabinetoffice.gov.uk/secretariats/committees/im.asp

145 Ev 110

146 Ev 111

147 Ev 110

148 Ev 110

149 Ev 85

74. In oral evidence, the Minister, Joan Ryan, explained that it was not correct to say that "there is no interaction between our eBorders development team and the ID card scheme because there is and it is very important. I am not sure the relationship between what is being developed in both these things is as close as the relationship with UK Visas and biometric residents' permits".[150] Evidence also raised concerns that there was unnecessary overlap between the identity card programme and the National Smart Card Project, which was established by ODPM in November 2002. This project will use smart cards to identify people in the following situations: gaining access to buildings, proving entitlement to benefits, recording transactions and making payments. It is envisaged that smart cards, without biometric details, will be used to access services such as education, libraries and leisure facilities. In relation to the National Smart Card Project, the ALCO Group Limited has said that "the ODPM's Government Connect project has to follow a parallel track to the ID card which is both wasteful on cost and will be confusing for citizens".[151] The Home Office responded to written questions regarding its interaction with Local Government regarding smart card technologies by stating that they have discussed common interest such as transaction authentication levels with the National Smart Card Project and Government Connect.[152]

75. The second, and perhaps more pressing, area of concern is the co-ordination of the scheme across Government and the risk posed to the technological success of the scheme by function creep. As already noted, the Home Office has not clarified the scope of the scheme or the ways in which the card might be used (paragraph 43). Furthermore, several external organisations have raised concerns regarding cross-departmental co-ordination and communication in relation to the scheme. The LSE has noted that "Since it was first proposed in 2002, the Identity Cards proposal has failed to win universal support amongst central government departments".[153] Nick Kalisperas from Intellect said in oral evidence that "what we have here is a reflection of the silo mentality that exists with the public sector. What we have here is the Home Office procuring a national identity card scheme but only within the boundaries that the Home Office can do".[154]

76. When this issue of cross-departmental interaction on the identity cards programme was raised in oral evidence, the departmental Chief Scientific Adviser, Professor Paul Wiles, did not answer, regarding it as "an implicit policy question".[155] Professor Wiles did at least acknowledge that "there is an important issue here about interoperability and whether we can ensure there is interoperability".[156] This point was underlined by the Minister, Joan Ryan. She said that "it is absolutely crucial that interoperability exists".[157] She emphasised that across Government the e-Government unit and the Government's Interoperability Framework will ensure interoperability. However, given that the scope or

150 Q 1186

151 Ev 109

152 Ev 124

153 Ev 91

154 Q 494

155 Q 1133, HC 900–x, (to be published in HC 900–II, Session 2005–06)

156 As above

157 Q 1185

use of the card within different Government departments does not yet seem have been finalised it is difficult to see how the scheme will be truly interoperable (see paragraph 41). It is more likely that other departments will have to fit into the scheme as developed by the Home Office. As explained by Intellect, the result is likely to be "a card that is very much reflective of the Home Office's own objectives and aims".[158] It is crucial that the scheme has a level of interoperability across Government and that technical specifications are able to interface. It is also important that the functions of the identity card are clarified as soon as possible across Government. During these discussions, the Home Office should also discuss the technological aspects of the scheme with other departments as well as the aims of the project. **We recommend that the Home Office undertakes a cross-Government consultation regarding its plans for technology to support the identity card scheme before the specifications of the scheme are finalised and that it makes the findings of this consultation public.**

International models

77. Several countries already use biometrics within identity card schemes. Greece, Italy, Portugal, Spain, Hong Kong and the Philippines for example collect one or more fingerprints as part of their national identity card schemes. These countries illustrate the trend towards the use of biometrics in travel and other identity documents (see paragraph 20). As the use of biometrics grows, the potential sources of scientific, technical and practical advice also increases.

78. The identity cards programme team has sought advice internationally, in particular from the US, Hong Kong and the Philippines. This has involved visits to these countries, meetings and ongoing dialogue.[159] It has also used evidence on biometric technology from one of the world-leading institutes, the National Institute of Standards and Technology in the United States.[160] In oral evidence, Nigel Seed explained that the identity cards programme team were considering the scalability of the project by comparing it to other systems. He noted that "The FBI fingerprint database has something like 45 million records, so the number you can process are up there. The UAE has got in excess of a million records on iris. We know these large projects can work".[161]

79. There is little information publicly available regarding the performance of other large-scale biometric projects. Professor Angela Sasse from University College London said in relation to the United Arab Emirates (UAE) iris scanning scheme, that "there have been no observed, properly controlled trials where we would have the figures that we can work on. We basically have to take on trust what they are saying".[162] Furthermore, the value of such advice is obviously limited according to the comparability of the schemes. The UK is the first country to introduce a nationwide scheme using three biometrics. Dave Birch from Consult Hyperion said that "The UK is in a very different situation. Most of the countries that are rolling out what you would call smart identity cards…already have some form of

158 Q 494

159 Ev 119

160 Ev 112

161 Q 334

162 Q 556

ID card they are upgrading, so it is not transparently obvious that the lessons you would pick up could automatically be applied in the UK".[163] We also note that the success of different schemes varies according to cultural and social norms of different countries. For instance, acceptable behaviour in the UAE in recording or verifying biometrics might not be acceptable in the UK. Thus information from the UAE iris scanning scheme may not be applicable to the UK. Professor Angela Sasse explained in oral evidence that:

> "the social and cultural context in those countries may not be exactly the same as in the United Kingdom, so certain behaviour that might be required from the citizen user in order to make the systems operate that may be perfectly acceptable there may not be acceptable to the citizens of the United Kingdom, and that aspect has not been looked at in a great amount of detail."[164]

80. Dr Tony Mansfield from the National Physical Laboratory agreed that "the environment, the population that is using the system, have a strong influence on the performance and the way these systems will work, so it does not matter how closely we look at other large schemes; it does not necessarily tell us exactly what would happen with biometrics on the United Kingdom scheme".[165] **We recommend that the Home Office continues to develop international links during the programme but stress that the limitations of advice and evidence from other schemes must be recognised by Ministers in the light of the unprecedented scale, the use of multiple biometrics and the complex IT requirements of the UK scheme.**

81. We also note an apparent discrepancy between the advice offered to us during our visit to the United States in March 2006 and the advice subsequently provided to the identity cards programme team. On 6 March 2006, we met informally a group of senior policy advisers from the Department of Homeland Security to discuss the identity cards programme. When questioned about the maturity of biometric technologies, the advisers agreed that currently the technology was probably not as reliable or as accurate as it might need to be for a national identity card scheme. We put these views to Katherine Courtney during an oral evidence session and she declined to comment on what we had been told.[166] The Home Office subsequently wrote saying that during a visit to the US in April 2004, officials put these views to senior advisers responsible for the operation, development and management of the US-Visit programme who rebutted them strongly.[167] Our visit to the US illustrated to us the ground-breaking nature of the UK scheme. **In order to build public confidence in the technologies involved, we recommend that the Home Office publishes an overview of the scientific advice and evidence that it receives as a result of international co-operation.**

163 Q 510

164 Q 556

165 Q 558

166 Q 272

167 Ev 119

5 The evidence base

Trials

82. In oral evidence to the Committee, Katherine Courtney emphasised that trials would commence once Royal Assent had been granted and the procurement phase had begun. She explained that the specific solution for the identity cards scheme could not be trialled until the bidders were given an opportunity to propose their ideas.[168] Furthermore, she stated that "we will be putting information about the plans for trialling into the public domain once we are able to begin the procurement process".[169] However we received more detail from the Home Office in response to subsequent written questions. The Home Office said that it will undertake three main tests:

a) a competitive trial of bidders' proposed solutions involving the live enrolment and verification of approximately 3000 people;

b) a large-scale matching test using pre-recorded biometrics that will provide statistical information on the relative performance of different solutions; and

c) a large-scale live enrolment to confirm that the solution will be capable of performing when the National Identity Register is fully populated.[170]

The Home Office also told us that these trials would provide "vital new information on fingerprint performance, - large scale performance, verification performance, enrolment and image quality, spoof resistance, usability and inclusivity".[171]

83. **We welcome the Home Office's commitment to publicising fully its plans for trialling once the procurement process has begun. In order to continue this move towards transparency and to build public confidence in the scheme, we recommend that the Home Office also makes public the results of these trials.**

84. It is anticipated that the trials will take place during the procurement process, which is expected to last between 15 and 18 months. In oral evidence to the Committee, Katherine Courtney stated that "we have made the assumption that the process of procurement, including the trials, will take somewhere between 15 and 18 months in order to make sure that we are giving sufficient time to operate those trials as part of that procurement process".[172] Furthermore, we acknowledge that the Home Office has stated that it will not be rushed. Katherine Courtney stated that "from the very first policy announcement when the Secretary was quite clear that there would be no big bang implementation of this scheme. That gives us lots of opportunity to test and ensure that we are getting things right".[173] The Minister, Joan Ryan, also noted that the future timetable of the scheme would

168 Q 331

169 Q 324

170 Ev 113

171 As above

172 Q 326

173 Q 310

be determined by the procurement process.[174] She said that the timetable is relatively loose because the Home Office wants to be "very cautious on the basis of all the lessons we have learnt from good and bad projects".[175] **We welcome the Home Office's cautious incremental approach and we encourage the Home Office, if necessary, to extend the procurement phase to ensure that enough time is taken to gather the necessary scientific evidence and to undertake all the appropriate trials. In view of the potential adverse impact on large numbers of people, it is better that the scheme is late and workable than on time but flawed.**

85. It is not only important that the Home Office allows enough time for trialling the technology but that time is built into the programme to allow for the results to be fed back into the proposed solutions. Professor Anne Anderson from Glasgow University has noted that "sufficient time must be included to refine the design in the light of evidence from realistic trials of the system in operation. It will be important to ensure that the relevant expertise is available to gather and analyze this data on the whole system performance".[176] **We recommend that the Home Office publicly outlines the ways in which the results of the trials have influenced and changed the programme.**

86. The Home Office has provided us in confidence with the details of the budget that has been allocated to trialling the technology supporting the identity cards scheme. Whilst we note that resources have been allocated specifically to trials, we would be concerned if this budget created a costs ceiling that will limit the trials that can take place. If the trials deliver unexpected results, it is imperative that further trials can be undertaken to explore such results in more detail. **We seek assurance that the Home Office will not limit the number, scope or quality of technology trials in order to stay within the allocated budget. We recommend that the Home Office ensures that sufficient funding is available to undertake the necessary technology trials for this scheme and that it retains flexibility regarding the trials that may be required.**

Biometrics

87. The Home Office has stated that it will use fingerprints, facial recognition and iris scanning in the identity cards scheme. As already mentioned, the specific solution has not been trialled and the Home Office intends to run operational testing of the technical systems during procurement. However, several trials have taken place to test the biometric technology. The Home Office states that trials have taken place on the performance of facial recognition systems, the capability of facial and iris systems to resist spoofing attempts and 'benchmarking' of a fingerprint system.[177] The facial recognition tests started in November 2005 and are still underway. The tests on iris systems took place in early 2006 at the National Physical Laboratory and the fingerprint system benchmarking was completed early in 2006.

174 Q 1144

175 Q 1145

176 Ev 120

177 Ev 113

88. In 2004, the identity cards programme team, the UK Passport Service (UKPS) and the Driver and Vehicle Licensing Agency (DVLA), commissioned Atos Origin to run a biometrics enrolment trial to gather evidence on public perceptions and attitudes towards biometrics. The Home Office has repeatedly asserted that this trial was not an assessment of the technological capabilities of biometrics. The report noted that "testing of the biometric technology itself was not one of the objectives of the Trial, rather the Trial aimed to test and measure the processes around recording and verification of biometrics".[178] As will be discussed in the chapter on public engagement, the status of the trial caused confusion and there were numerous press reports detailing the apparent problems with the technology (see paragraph 138). This confusion has perhaps been exacerbated by the Home Office's treatment of the results from the trial and their inconsistent use of it as evidence. When questioned in an oral evidence session about the false non-match rates that resulted from the Atos Origin trial, Katherine Courtney said that "I think it is important to reiterate that the enrolment trial was a trial of process and customer experience. It was not designed as a trial to look at performance of the technology *per se*".[179] However, the results of the trial have been used to provide information about technology performance. On 29 June 2005, despite noting that the Atos Origin trial was not intended as a test of technology, the then Parliamentary Under-Secretary for Immigration, Citizenship and Nationality, Andy Burnham used statistics from the trial in order to answer a question relating to the failure to acquire rate of the technology.[180] **There is evidence that whilst trial plans were set out clearly the processes with which they were enacted lacked rigor. As a result, the Home Office has selectively used evidence from the biometrics enrolment trial to support its assertions. We believe that the Home Office has been inconsistent regarding the status of this trial and this has caused confusion in relation to the significance of the evidence gathered about biometric technologies. We recommend that the Home Office clarifies whether or not it accepts the validity of the results gained during the trial regarding the performance of biometric technologies.**

89. Furthermore, even though the biometrics enrolment trial was not devised as a performance trial, it highlighted problems with the technology. For example for iris enrolment, success at the first attempt was higher for asian and white participants than black participants.[181] Tony Mansfield from the NPL said that "it illustrated that if you buy off-the-shelf systems and deploy them with no adaptation to the ID cards programme the performance would not be terribly good…clearly the performance was inadequate in that trial."[182] **Given the findings of the biometrics enrolment report regarding the performance of current biometric systems, we seek reassurance from the Home Office that systems will be adapted as necessary to improve performance levels and that final performance levels will be verified by independent testing.**

178 UK Passport Service/Atos Origin, *Biometrics Enrolment Trial,* May 2005, p 8

179 Q 299

180 HC Deb, 29 June 2005, Col 1572W

181 UK Passport Service/Atos Origin, *Biometrics Enrolment Trial,* May 2005, p 42

182 Q 573

90. The Home Office may have turned to the biometrics enrolment trial report to support its assertions regarding facial recognition technology due to a lack of information from other sources. Given the uniquely ambitious nature of the UK identity cards scheme, there is no independently-validated evidence regarding performance levels either from existing systems or from large-scale trials for the biometric technology involved in the scheme. The written evidence submitted by the LSE highlights that "the biometric technology at the core of the scheme has been untested at the scale proposed by the Home Office".[183] Indeed, the Home Office acknowledges that for iris scanning "no independent testing on databases of millions has been undertaken to date".[184] Neither is there a large-scale database for multimodal biometrics.[185]

91. Despite this lack of information regarding the performance of biometric technologies, the Home Office provided us with performance levels from existing evidence that would be "consistent" with their requirements (see paragraph 18).[186] The performance levels were taken from five different reports produced by four organisations over a period of four years.[187] Data relating to the performance of iris scanning relied upon unpublished, unverified results from the Schipol airport trial and the UAE iris system. The Home Office did note that "the data were not collected under the same conditions so caution should be used in interpreting these figures".[188] We are surprised by the Home Office's unscientific approach and suggest that rather than collating figures merely to provide information regarding performance, the Home Office admits that it cannot release details until it has completed trials. **We note the lack of independent evidence relating to the performance of iris scanning and welcome the Home Office's commitment to undertake a large-scale matching test using pre-recorded biometrics. Given the relative lack of information available publicly regarding the performance of biometrics in a national scheme, we recommend that once the scheme is established the Home Office publishes details of the performance levels of the technology.**

92. In light of the lack of evidence relating to the large-scale use of multimodal biometrics, we are concerned that, although the exact biometrics are not specified in the Identity Cards Act 2006, the Home Office has already fixed the number and type of biometric that will be used. The Home Office apparently made the initial decision to use face, iris and fingerprint biometrics by assessing the available existing scientific evidence. Katherine Courtney stated in oral evidence that "when we reviewed all the literature, the research, also the practical experience from programmes around the world, we looked at systems that did use more than one biometric".[189] Qinetiq has questioned the breadth of this research stating that "a

183 Ev 87

184 Ev 57

185 As above

186 Ev 111-112

187 P. Jonathon Phillips, Patrick Grother, Ross J. Micheals, Duane M. Blackburn, Elham Tabassi & Mike Bone, *Face Recognition Vendor Test 2002* (March 2003); Tony Mansfield, Gavin Kelly, David Chandler & Jan Kane, *Biometric Product Testing Final Report* (19 March 2001); C.L. Wilson, M.D. Garris & C.I. Watson, "Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints", *NISTIR 7110* (May 2004); Charles Wilson et al, "Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report", *NISTIR 7123* (June 2004); International Biometric Group, *Independent Testing of Iris Recognition Technology* (May 2005)

188 Ev 112

189 Q 291

single report from the National Physical Laboratory—valid though it was—was the sole justification for using three biometrics".[190] This report, the *Feasibility Study on the Use of Biometrics in an Entitlement Scheme*, produced by Tony Mansfield from the NPL and Marek Rejman-Greene from BTExact Technologies stated that combining biometrics "can improve performance…however the performance improvement is unlikely to be commensurate with the increased costs".[191] Furthermore, the research underpinning the Home Office's decision appears to have been theoretical rather than practical and the identity cards programme is still gathering evidence regarding the impact of multiple biometrics. When giving oral evidence to the Committee, Katherine Courtney stated that "the function for us of the multiple biometrics…needs to be tested during the procurement process in order to ensure that we have gathered the evidence base, that those biometrics will enhance the performance of the system".[192]

93. **We are surprised and concerned that the Home Office has already chosen the biometrics that it intends to use before finishing the process of gathering evidence. Given that the Identity Cards Act does not specify the biometrics to be used, we encourage the Home Office to be flexible about biometrics and to act on evidence rather than preference. We seek assurance that if there is no evidence that any particular biometric technology will enhance the overall performance of the system it will not be used.**

Information and communication technology

94. With regard to ICT, we note that the ICT systems have not yet been trialled. Evidence taken by the Committee from the ICT community recommended that the ICT solution should be trialled. Nick Kalisperas from Intellect said that "it needs to be piloted and then rolled out gradually."[193] Professor Martyn Thomas from the UKCRC agreed and emphasised that "the purpose of that would be to discover the weaknesses, the things that had gone wrong, and therefore you would need to allow plenty of time and plenty of budget for backtracking, for making modifications, perhaps for radical revisions of the scheme".[194] Although the Home Office has asserted that it intends to roll out the scheme gradually, it is not clear how it will do this.

95. **We note the lack of explicit commitment from the Home Office to trialling the ICT solution and strongly recommend that it take advice from the ICT Assurance Committee on trialling. We seek an assurance that time pressure and political demands will not make the Home Office forgo a trial period or change the purpose of the scheme.**

190 Ev 86

191 Tony Mansfield & Marek Rejman-Greene, *Feasibility Study on the Use of Biometrics in an Entitlement Scheme,* February 2003, p 12

192 Q 292

193 Q 505

194 Q 506

Research and development

96. In written evidence the Home Office said it was not necessary to embark on publicly-funded scientific research to improve the capabilities of biometrics.[195] This claim was subsequently denied in oral evidence and the identity card team asserted that research was being undertaken into fingerprint biometric performance. Katherine Courtney said "I would not say that we have not commissioned research. We have commissioned research. We have a piece of research that the Home Office is funding right now into fingerprint biometric performance".[196] We regret the confusion at the Home Office regarding the research that it is funding and what research it requires. The Government Chief Scientific Adviser's *Guidelines on Scientific Advice in Policy Making* state that departments should "think ahead and identify early the issues on which they need scientific advice…and where the current evidence base is weak and should be strengthened".[197] The Home Office has not provided us with evidence either that they have identified areas where the evidence base is weak nor that they have commissioned research in order to strengthen it. On the basis of the evidence that we have seen, we conclude that the Home Office does not seem to have an effective mechanism for ensuring that the required research and development in the relevant scientific and technological areas is carried out. **We recommend that the Home Office identifies the gaps in the evidence base underpinning the identity cards programme, that it commissions research to fill these gaps and that it feeds any new developments into the scheme where appropriate. This process should be overseen by the departmental Chief Scientific Adviser.**

97. The technological fields that will support the identity cards programme are constantly developing. Katherine Courtney acknowledged that "The field is evolving all the time. I think one of the challenges has to be to design a system that is flexible enough possibly to accommodate advances in the technology later down the line".[198] In relation to horizon scanning, the Home Office said that it would encourage the consortium that won the contract to take advantage of any new knowledge in the area. Marek Rejman-Greene, Head of the Biometrics Centre of Expertise, stated that "During the course of the deployment and early years of the programme, we would certainly ensure and ask the consortium that was winning the project to take advantage of that knowledge and home in on it".[199] Even if horizon scanning activities were already embedded in the identity cards programme, we would seek assurance that these activities fed back into the scheme. We note that the departmental Chief Scientific Adviser, Professor Paul Wiles, stated that with regard to the Home Office in general, "getting an organisation to actually lift its head from immediate problems and think ten or twenty years ahead and use that horizon scanning is sometimes a challenge".[200] We welcome Professor Wiles' admission and emphasise that it is part of the departmental Chief Scientific Adviser's job to ensure that this challenge is met by Ministers. We will return to this issue of research and horizon scanning in the overarching

195 Ev 51

196 Q 331

197 HM Government, *Guidelines on Scientific Analysis in Policy Making,* October 2005, p 2

198 Q 291

199 Q 303

200 Q 1105, HC 900–x, (to be published in HC 900–II, Session 2005–06)

report on scientific advice, risk and evidence. **The Home Office cannot afford to delegate responsibility for horizon scanning to others. We recommend that the Home Office actively undertakes horizon scanning activities relevant to the technologies involved in the identity cards programme and that it develops mechanisms to feed this information back into the scheme.**

98. During the inquiry, the identity cards programme team displayed an apparent reliance on existing research, which although broadly relevant to the programme does not necessarily deal with the specific challenges of the project. Whilst we identified earlier the ways in which existing research had been used in the field of biometrics (paragraph 92), the same issues occur in relation to ICT. For example, in oral evidence to the Committee, Nigel Seed claimed to have studied the Royal Academy of Engineering and British Computer Society report on *The Challenges of Complex IT Projects* (see paragraph 60).[201] We have several concerns regarding this statement. We would welcome it if the Home Office was following best practice as detailed in *The Challenges of Complex IT Projects* report. However, despite requesting it, we have not received detailed evidence from the Home Office that supports Nigel Seed's claim.[202] Secondly, this report does not in itself provide a detailed guide of how a major project should be managed. Finally, whilst it is vital that the Home Office learns the lessons outlined by this report, the report is also not a substitute for funding research specifically related to the identity cards project. **We urge the Home Office to commission, and where appropriate fund, research focused on the specific requirements of the information technology systems in the identity cards scheme rather than relying on general existing study results.**

Technology and operating costs

99. As already mentioned, the question of the cost of the identity cards scheme has caused fierce debate both within and outside Parliament. As a result, the Identity Cards Act 2006 requires a six monthly report on costs to be brought before Parliament.[203] The Home Office has repeatedly stated that the total year-on-year running costs of the scheme, primarily relating to people and services, would be £584 million. Katherine Courtney said to us that "We are quite confident in our cost estimates".[204]However, the Home Office has not released meaningful estimates within this figure. In December 2005, the-then Minister Andy Burnham said that "the estimates are…commercially sensitive and to release them may prejudice the procurement process and the Department's ability to obtain value for money from potential suppliers".[205]

100. The costs outlined by the Government were challenged by the LSE in its Identity Project Report. The LSE estimated that the scheme's implementation and running costs would be in the range of £10.6 billion to £19.2 billion during first ten years of the scheme.[206]

201 Royal Academy of Engineering & British Computer Society, *The Challenges of Complex IT Projects*, April 2004

202 We note that in oral evidence Dr John Daugman said that this Report was "a big part of the brief that has been given to the members of the Biometric Assurance Group" (Q 553)

203 *Identity Cards Act 2006,* section 37

204 Q 360

205 HC Deb, 7 December 2005, col 1362W

206 LSE, *The Identity Project Report*, June 2005, p 247

The discrepancy between the LSE and Government figures caused prolonged, and at times hostile, debate. The written evidence submitted to us by the LSE acknowledges that the discrepancy in figures between their estimates and the Home Office estimates results in part from what is included. The LSE states that "Our figures always included set-up costs, running costs and costs of integration with other Departments. The Home Office figures…are 'The current best estimate for the total average running costs'".[207] Katherine Courtney also pointed out to the Committee that "the costs modelling behind the LSE made a number of fundamental assumptions which were very different to our own proposition".[208] However, in oral evidence Dr Edgar Whitley from the LSE still said that "On the basis of no technology trials or limited technology trials and specifications still being changed I just cannot see how they can be so clear that it is £584 million".[209] We have no wish to guess the true costs but it is difficult to believe that such a certain figure can be established when there are so many variables.

101. The Home Office figures were audited by KPMG.[210] The Home Office has interpreted this audit, which was published in November 2005, positively. In a report on the KPMG review, the Home Office stated that KPMG "confirmed that the majority of cost assumptions within their scope were based on appropriate benchmarks and analysis from the public sector and suppliers".[211] In oral evidence, Katherine Courtney stated that, "our cost assumptions have been independently audited by KPMG and so we can have quite a high degree of confidence in them at this point in the development of the scheme".[212]

102. However, the audit highlighted some potential problems with the scheme. Despite Government assertions that a 10-year card life would be feasible, KPMG found that supporting information from suppliers was inconclusive.[213] KPMG stated that "the durability of the cards over the ten year period is questionable" and it recommended that the Home Office revise its cost estimates accordingly. [214] KPMG also noted that:

> "the performance of the biometric matching drives a significant amount of cost […] the IDCP [identity card programme] team should have further discussion with the USVISIT programme to gain detailed insight into the cost drivers for this area and the UAE [United Arab Emirates] to verify the cost and performance of the fingerprint and iris hardware matchers respectively".[215]

When questioned on 22 March 2006 about whether the identity cards team had followed this suggestion, Katherine Courtney admitted that they had not yet done so.[216] Our

207 Ev 91

208 Q 362

209 Q 570

210 KPMG, *Cost Methodology and Cost Review* , 7 November 2005

211 Home Office, *Summary of work in progress on areas of the ID Cards Scheme highlighted by the KPMG Review*, November 2005, p 1

212 Q 360

213 Home Office, *The London School of Economics' ID Cards Cost Estimates & Alternative Blueprint* , July 2005, p 2

214 KPMG, *Cost Methodology and Cost Review* , 7 November 2005, p 9

215 As above, p 11

216 Q 369

concern that the identity cards programme still has to gather evidence regarding the performance of multimodal biometrics is compounded by the fact that they are also not apparently exploring the relationship between performance levels and cost (paragraph 90). We also note that Intellect has said that "It is imperative that the Government selects a solution that is proven to work, and not one that is selected solely on the grounds of cost".[217] **We recommend that the identity cards programme team returns to the KPMG audit report and implements its recommendations. Furthermore, we re-emphasise that the Home Office needs to work out how costs will impact on performance and we seek reassurance from Government that cost limitations will not compromise the level of performance that is accepted.**

103. Despite the release of figures regarding the running costs of the project, there is still a lack of clarity concerning the start-up costs and specifically the costs of the technology within the project. We agree with Professor Angela Sasse's comment that "We have not been given enough detail to really check the validity" of costings.[218] We do not share the Home Office's belief in their costings given that the breakdown of technology costs provided to us in confidence only provided a broad overview and did not include any figures.[219] In the light of this lack of evidence, we can only conclude that the Home Office is not confident in its figures and as a result, we are incredulous that the Home Office is seemingly able to produce firm costings regarding the running costs of the scheme when the costs of the technology are not yet clear.

104. As well as assessing the costs of the scheme, the Home Office has undertaken work to assess the benefits of the identity card programme.[220] This research considered the strategic benefits for example in the delivery times of services, quantifiable benefits such as improved crime detection and non-quantifiable benefits like convenience. It found that "Most organisations have at present only been able to model more conservative, incremental changes that would result from ID cards. Even with these constraints, the quantified, financial benefits range from £650m to £1.1bn per annum when the scheme is fully rolled out".[221] As the scope of the scheme is finalised, we encourage the Home Office to update its research regarding the benefits, as well as the costs, of the scheme.

105. **We are sceptical about the validity of costs produced at this early stage. We acknowledge that the release of firm overall costing has been driven by political imperatives but the Home Office could have credibly given a broad range instead of precise figures. We note the danger that a desire to keep below a costs ceiling might drive the choice of technology. We seek assurances that the costings are flexible. We strongly recommend that, once the procurement process has taken place, the Home Office publishes a breakdown of technology costs, including set-up costs, running costs and predicted savings as a result of the scheme in the Home Office and elsewhere.**

217 Ev 103

218 Q 570

219 Ev 117

220 Home Office, *Identity Cards Scheme– Benefits Overview,* June 2005

221 As above, p 1

Social science

106. The Home Office has undertaken nine pieces of social science research in 2004 and 2005. This research included:

a) omnibus research, which was carried out in February, April, October and December 2004;

b) qualitative research on "special needs issues" and "citizen's views on proposed customer propositions", which was completed in December 2004; and

c) two pieces of quantitative research on UK citizens' and user organisations' views on the scheme, and foreign nationals' views on the scheme. This work was published in October and December 2005.[222]

In oral evidence to us, Professor Angela Sasse said that she thought that the Home Office became aware of the societal impact of the scheme during the Home Affairs Select Committee investigation in 2004.[223]

107. We welcome the work that the Home Office has undertaken in the area of social science research. We have also received evidence that suggests that the scope of this research could be broadened. Professor Anne Anderson from Glasgow University has stated that "although this input from social science may well have been valuable to the…National Identity Scheme, it is a narrow perspective on social science and where the social sciences could be used to improve the scheme".[224] Furthermore, she notes that "the National Identity Scheme is a very challenging project. It is a complex socio-technical system and to be effective will require that the Home Office considers the social as well as the technical dimensions".[225]

108. Professor Anderson also notes that ICT systems often fail to deliver benefits because the systems have been designed without understanding about the context of use or users' needs. She further states that "the challenges of implementing the various biometric technologies have been the focus of concern, and it appears that less attention has been given to the challenges of how to design and implement the system in ways that are usable, useful and appropriate".[226] The ways in which the identity card scheme would function vary depending on whether members of the public or service providers are the prime users and beneficiaries of the scheme. If the former, then there might be recognition of the views of different users regarding the amount of information made available to the service provider. Professor Anderson highlights the positions of individuals such as celebrities, those being stalked or those leaving abusive relationships. The matter has also been raised regarding the ways in which an identity card might be used by those with mental health problems or those that are blind.[227] In general, Professor Anderson notes that "The key

222 Ev 117; British Market Research Association, *What is an Omnibus Study?,* October 2002, www.bmra.org.uk

223 Q 549

224 Ev 120

225 Ev 121

226 Ev 120

227 Qq 549-550

point I want to make is that the Home Office needs to be more sensitized to these social concerns".[228]

109. We have noted that the identity card proposals have been firmed up since the earliest studies.[229] For example, from 2010 the cards will be compulsory, the Identity and Passport Service has been created and the minimum age has been set at 16. Furthermore, we note the complexity of the social concerns regarding identity cards highlighted briefly by Professor Angela Sasse and Professor Anne Anderson. **We recommend that the Home Office prioritise funding as necessary to ensure that required social science research is undertaken and if necessary commissioned. In particular, we emphasise the need to undertake work to understand the attitudes of prime users towards the current proposals.**

110. In response to written questions, the Home Office explained that advice on social science is derived from different sources dependent upon its nature. Statistical advice is provided by the Research Development and Statistics (RDS) unit within the Home Office; advice on research requirements is given by the Marketing and Communications team within the Identity and Passport Service (IPS), and advice on commissioning research is provided by the Central Office of Information.[230]

111. Within the identity cards programme, large pieces of social science work have tended to be commissioned from private companies, rather than being undertaken in-house.[231] We recognise that commissioning externally may be more cost effective than maintaining an in-house capability, but there are disadvantages. As a result, social science work has seemed to focus upon one-off pieces of work rather than consistent monitoring. Furthermore, Professor Sasse has noted that this work is not necessarily followed up. She said in oral evidence that "there is a bit of a lack of depth and a lack of following-up on problems that have been discovered to see how they could be overcome".[232] **We recommend that the Home Office establishes a clear process by which advice from external social science experts regarding future research and the social science aspects of the programme can feed into the scheme. Once research has been undertaken, we urge the Home Office to develop the expertise that will allow it to follow up the results.**

228 Ev 121

229 Home Office, *Public perceptions of identity/entitlement cards* , January 2003; Cragg Ross Dawson, *Public Perceptions of Identity Cards: Qualitative Research Report,* August 2004

230 Ev 117

231 Cragg Ross Dawson, *Public Perceptions of Identity Cards,* August 2004; TNS Consumer, *Awareness, Understanding and Attitudes to ID Cards,* September 2004

232 Q 550

6 The treatment of risk

Treatment of risk

112. The identity cards scheme faces a range of risks including technological problems, vulnerability of information, physical damage to systems, time delays and escalating costs. Given the potential for severe damage to public confidence in the scheme if these risks are not mitigated successfully, risk management is a key component of the scheme. The importance of risk management in large-scale ICT projects like the identity cards programme cannot be underestimated. The UK Computing Research Committee has stated that "poor risk analysis and risk management is repeatedly identified as a significant factor in the failure of public sector IT-enabled business change projects".[233] The LSE has noted that "the accumulated independent evidence on large complex IT projects is that they have been and always will be high risk in terms of implementation and unanticipated costs".[234]

113. The evidence that we have received from external organisations in relation to the Home Office's approach to risk management has varied. Qinetiq stated that "it is our view that the programme still contains considerable risk at this stage of procurement".[235] The LSE went further and asserted that "there is a significant risk that the technology will never work well enough in practice for a large-scale public domain application, and large amounts of money will be lost if this is discovered too late in the project".[236] However, other groups have disagreed. The British Computer Society (BCS) has said that "within the ID arena [risk analysis] seems to have been successful" and the National Physical Laboratory has affirmed that "risk is being appropriately considered".[237]

114. The Home Office has asserted that it is following best practice with regard to risk management. The Identity and Passport Service Programme Control Office Risk Management team is embedded in the identity cards programme and its policy draws on advice from the Office of Government Commerce Management of Risk, the HM Treasury Orange Book, the Institute of Risk Management and the Government Communications Head Quarters (GCHQ).[238] This policy involves identifying all risks as early as possible and providing them with a named owner, who is given advice by a risk manager. The owner assesses the probability of the risk occurring and its likely impact on budget and schedule. This information is entered into a programme risk tool that calculates an overall score, which it uses to prioritise the risk. The risk owner then decides how to approach the risk, for example transferring it, tolerating it, terminating it or treating it. If possible, the risk is mitigated. The details of these risks and their mitigation are entered into a risk register.[239]

233 Ev 76

234 Ev 90

235 Ev 86

236 Ev 91

237 Ev 82, 110

238 Ev 118

239 Ev 123

115. As part of this risk management strategy, the Home Office also undertakes contingency planning. The Home Office has told us in response to written questions that "Contingency planning is not done for every risk but will be done, in line with accepted practice, chiefly based on the severity of the post-mitigation status and overall risk score for the risk".[240] The Home Office appears to be confident in this process. The Minister, Joan Ryan said that "I am not anticipating something major that would completely delay or derail the programme".[241]

116. Despite repeated requests from the Chairman of this Committee to view the relevant sections of the risk register in confidence, the Home Office has not granted us sight of the risk register because of its sensitivity at this stage in the programme. The Minister, Joan Ryan, said that "there are potential confidentiality issues around parts of the risk register and obviously, at the point we go into procurement, this is crucial."[242] Instead, on 10 July 2006 the Home Office provided presentations that gave an overview of their approach to risk management and used examples of risk management from within the programme (see paragraph 5). These examples give us a level of confidence in the Home Office's risk management strategy but we note that we only discussed a selection of risks. We were surprised that the Home Office was not content for us to list the examples that we discussed, even without reference to risk level or risk treatment.[243] We do not believe that the Home Office's caution on this occasion was justified and the incident exemplifies the closed nature of the identity cards programme. **The Home Office has provided us with details of the risk management strategy within the identity cards programme. However we are disappointed that the Chairman was not allowed to view the risk register in confidence. In the light of the evidence provided to us, we are somewhat reassured by the Home Office's risk management strategy. Any delay to the procurement process will postpone the treatment of various risks. We seek assurance that the timing of the procurement process will be considered in relation to risk management.**

117. We note concerns from external bodies that highlight that information regarding risk management within the identity cards programme has not been made public. Microsoft has stated that "during the present phase of consultation the risk model has not been made publicly available".[244] We accept that the Home Office may not wish to make the exact risks encountered by the project public for security reasons. However, we think that the identity card programme could benefit from a wide-ranging discussion regarding risk management strategy before entering the procurement process. **We recommend that the Home Office make details of its risk model public and that it takes steps to ensure that advice regarding risk management can feed into that model.**

118. The identity cards programme has undertaken several Office of Government Commerce Gateway (OGC) Reviews. These Reviews independently examine acquisition programmes and procurement projects at critical stages in their lifecycle. There are five OGC Gateway Reviews during the project lifecycle: three before contracts are awarded and

240 Ev 123

241 Q 1175

242 Q 1161

243 Ev 129

244 Ev 127

two focusing on service implementation. The OGC Gateway Review 0 is a programme-only review that is repeated throughout the programme's life and it can be applied to policy implementation, business change or other types of delivery.[245] The House of Commons Public Accounts Committee undertook an inquiry in November 2005 on the OGC Gateway Review process. It found that the process had succeeded in "bringing more rigorous scrutiny and oversight to IT-enabled programmes and projects, and providing the means to highlight risks sufficiently early for senior management to take recovery action".[246] As a consequence, we have confidence in the Gateway Review process. The identity cards programme has undertaken the following reviews:

Gateway Zero (Strategic Assessment) completed 30 January 2004

Gateway One (Business Justification) completed 18 July 2005

Gateway Zero (Strategic Assessment) completed 14 January 2006

Gateway Two (Procurement Strategy) completed 11 April 2006

119. We acknowledge that these reviews remain confidential in order to ensure that participants are fully open regarding the actions that are needed in order for a programme to proceed to the next stage.[247] However, outside the programme the lack of information regarding the Gateway Review process has generated concern, which has been heightened by recent press reports containing information from the OGC.[248] The Local Authority Smartcard Standards e-Organisation (LASSeO) has stated that "presumably the project has been through some kind of gateway process but this remains unclear outside the project".[249] **We recommend that an overall indication of the outcomes of the OGC Gateway Reviews, but no specifics, be made public in order to increase confidence in the scheme.**

120. One of the serious risks faced by the identity cards project is that time pressures will prevail and the scheme will be rolled-out before it is ready. We have already described the Home Office's incremental, cautious approach to the scheme (see paragraph 10). The Minister, Joan Ryan said in oral evidence that "I do not feel I am running this according to some political deadline".[250] We are concerned however that earlier in the same session she said that "What we have been told is that there is a desire, and a strong desire, to see ID cards towards the end of 2008–09 being issued".[251] Moreover the Home Secretary, Rt Hon John Reid MP said to the House of Commons on 11 July 2006 that "I reaffirm our commitment to the introduction of those [identity cards] as rapidly as possible".[252] If a deadline is strongly desired, the Home Office might alter its currently cautious approach as

245 OGC Gateway Review 0: Strategic assessment, www.ogc.gov.uk

246 House of Commons Public Accounts Committee, Twenty-Seventh Report of 2004–05, *The impact of the Office of Government Commerce's Initiative on the delivery of major IT-enabled projects*, HC 555, p 1

247 Ev 115

248 "E-mails from Whitehall officials in charge of ID cards", *The Sunday Times,* 9 July 2006

249 Ev 94

250 Q 1174

251 Q 1159

252 HC Deb, 11 July 2006, col 1324

the deadline approached and in doing so, place the success of the scheme at risk. We also note that as the end of the current Parliament approaches, political pressure upon the scheme may increase. **It is important that the impact of a politically-imposed deadline will not override the impact of scientific advice or evidence on the readiness of the scheme and we seek reassurance from the Government on this point.**

121. In relation to biometrics, one of the key risks faced by the scheme is the presentation of false biometrics, "spoofing" (see paragraph 19). The Home Office acknowledged in written evidence that "It may be impossible to prevent applicants falsifying (spoofing) their biometrics. This risk can be mitigated through analysing the threat posed and designing the correct detection processes and by ensuring that the deterrent regime is appropriate".[253] Furthermore, the Home Office has stated that the identity cards programme team is working with experts from the Communications Electronics Security Group (CESG), the National Physical Laboratory and independent specialists.[254] They have also reassured us that resistance against spoofing will be part of any biometric testing during the procurement process.

122. Whilst biometrics obviously involve risks such as spoofing or unreliability of verification, it is important that the Home Office does not just focus on this field because it is an emerging technology. Dr Tony Mansfield from the National Physical Laboratory told us that "There seems to have been a focus on the biometric element as being the most technical and perhaps least understood element of the whole scheme, and to my mind assuming that is where all the risks lie is totally incorrect".[255] With regard to the identity cards scheme, it must be recognised that the ICT system, as well as the biometric technologies, involves risks. We emphasise that the cost of failure of this project would be great and the Home Office cannot afford to be complacent regarding any aspect of risk management. **We emphasise the importance of the development of an holistic approach to risk management in order to ensure that focus on biometrics as an emerging technology does not detract attention from other aspects of the scheme.**

ICT system

System architecture

123. Large-scale ICT projects are generally considered to be high-risk and numerous reports have highlighted problems with schemes similar to the identity cards programme. The Royal Academy of Engineering and British Computer Society Report, *The Challenges of Complex IT Projects*, said "it is alarming that significant numbers of complex software and IT projects still fail to deliver key benefits on time and to target cost and specification".[256] The Public Accounts Committee Report, *Achieving Value for Money in the Delivery of Public Services*, said that "IT projects have over the last ten years been prone

253 Ev 51

254 Ev 60

255 Q 553

256 Royal Academy of Engineering & British Computer Society, *The Challenges of Complex IT Projects,* April 2004, p 4

to significant problems which the Committee believe should have been avoided".[257] The Home Office has been associated with computer projects such as the police national computer, the UKPS ICT project and the asylum seeker processing system that have drawn criticism in the past.

124. In oral evidence however, several witnesses emphasised that the risk of a major ICT system going wrong could be mitigated and we note that several schemes such as the DVLA online car tax system or the HM Revenue and Customs online tax return system have been successful following some initial problems. Professor Martyn Thomas said that "UKCRC is increasingly frustrated by the fact that major IT procurements go wrong for entirely avoidable reasons".[258] Dave Birch from Consult Hyperion also said that "We get a lot of criticism about all of these projects continuously going wrong […] It is not just because we are IT people; it is because of the way these things are approached".[259]

125. The Home Office's current approach is to allow industry flexibility in producing a solution. In oral evidence Katherine Courtney said that the identity cards programme team is choosing "to focus on the outcomes we are trying to achieve and not dictate to the industry what the technical architecture should be".[260] The Minister, Joan Ryan, also explained that the technology that is developed through procurement will be driven by the outcomes required by the scheme. She denied that the Home Office would be hostage to the market, saying that in the first phase when prototypes or pilots are produced the market will bear the risk.[261] This approach presumes firstly that industry will be able to deliver an appropriate solution and secondly that the Home Office and its consultants have sufficient expertise to judge between the solutions proposed by industry. We are concerned that the Home Office may be leaving the design of the scheme up to the market, because it lacks the scientific expertise to be an intelligent customer. In oral evidence, Nigel Seed acknowledged "we are not the experts in the technology; they are".[262] Furthermore, the Minister, Joan Ryan said to us that "The private sector suppliers are the experts in developing the technology. We want to use their expertise and continually stretch them throughout the procurement process".[263] This issue has been raised in written evidence by Peter Tomlinson from Iosis Associates who states that "procurement by the public sector of ICT systems and services is today largely in the hands of people without expertise in this technology area, whereas until the early 1990s public sector purchasers of IT systems generally had the expertise".[264] It was echoed in oral evidence by Dave Birch from Consult Hyperion who said that "you have people who are, frankly, scientists giving evidence to people who are, frankly, not".[265]

257 Public Accounts Select Committee, Seventeenth Report of Session 2005–06, *Achieving Value for Money in the Delivery of Public Services,* HC 742, p 11

258 Q 488 (Thomas)

259 Q 488 (Birch)

260 Q 270

261 Q 1151

262 Q 276

263 Q 1150

264 Ev 98

265 Q 486

126. Although the Home Office has said that it will leave the solution to industry, industry representatives have expressed uncertainty regarding the extent to which the scheme will be prescriptive. Nick Kalisperas argued that "If you just say, 'We are going to leave it to the market' that is just too broad. There has to be the outlines of a specification there".[266] Dave Birch disagreed, saying that "It is not being left up to the market; it is in fact very prescriptive. It is already decided that there will be a smart card. It is already decided that there will be a register".[267] Jerry Fishenden from Microsoft responded that "there is something contradictory happening here" and noted that "the proof will be when the procurement documents come out and we can see how outcome–based it is and how prescriptive or not the actual procurement intends to be".[268] Either a non-prescriptive or prescriptive approach is valid as long as the Home Office makes its intentions clear. The apparent contradiction between the Home Office's assertions and its actions is causing confusion, which as already explained has been exacerbated by a lack of clarity regarding the terminology surrounding procurement (paragraph 46). We are disappointed that confusion regarding the specification of the scheme has arisen and we are concerned that, as mentioned earlier, the Home Office has not seemed to want to engage with industry regarding the architecture of the scheme before releasing the specifications (paragraph 30). **Industry is hoping that the commencement of procurement and the release of specifications will clarify the Home Office's position. Once the specifications have been released, we urge the Home Office to take steps to ensure that the specifications, requirements and risks have been clearly understood by all involved.**

127. The evidence has highlighted that in complex ICT schemes, it is best practice to develop a system architecture for the scheme as soon as possible. Professor Martyn Thomas from the UKCRC explained in oral evidence that:

> "in the same way as an architect sits between the client who wants a new major building, and works out with the client what the requirements will be, how the business will be affected by the new system that is being procured, in exactly the same way, you could have a system architect come in for major IT systems, to work in a very technical way with the potential suppliers but in a very business-oriented way with the client and do the translation, so that the architect would capture the business requirements and turn them into a very rigorous specification because they would be put out for competitive procurement."[269]

128. The written evidence submitted by the UKCRC said that "Systems Architects would be people with advanced skills in adopting rigorous approaches to software development and project evaluation".[270] Professor Thomas expanded upon this point in oral evidence, explaining that "system architects would typically come from the innovative smaller companies that are using the more advanced technology by doing things like requirements' analysis".[271] The points raised by Professor Thomas have previously been outlined by the

266 Q 489 (Kalisperas)

267 Q 489 (Birch)

268 Q 489 (Fishenden)

269 Q 487

270 Ev 75

271 Q 487

British Computer Society and the Royal Academy of Engineering report on *The Challenges of Complex IT Projects*.[272] This report emphasised that a systems architect should provide an overview of the technical structure of a scheme without detailing its implementation. It stressed that an effective IT architecture should be flexible, scalable and evolvable. Thus, the notion of setting an architecture for a scheme does not exclude a competitive and innovative procurement process. Furthermore, this approach overcomes the problems that can be faced by a department that lacks the right level of skills. Intellect has said that "system requirements that are inadequately explained and thought through in the procurement specification or changed during the process create an unacceptable burden, especially for smaller suppliers".[273]

129. We have not received clear evidence that the Home Office has considered this approach in ICT, although we note that a similar approach is being used in relation to business aspects of the scheme.[274] The Home Office has said that it is using a "modular IT architecture design approach" but has provided little more information.[275] In response to written questions, the Home Office has said that it is working with Qinetiq to explore "model technical architectures which are tolerant of high data volumes and variations in data volumes".[276] However, it also notes that neither the scope of this project nor its timescale are finalised. **The Home Office is reliant on external expertise in the area of ICT and is unable to act as an intelligent customer of scientific advice. We recommend that the Home Office uses a senior and experienced systems architect to advise on the specifications and to provide support during the procurement process.**

Security

130. The Government claims that the National Identity Register will be highly secure. In oral evidence to us, Katherine Courtney said that "I was intent on having the best security advice possible, and so we brought in not only the government security advisers but also other independent security advisers to work with us on this".[277] She emphasised that the scheme was already part of the critical national infrastructure and as such, it was being accredited by the Government's security advisers.[278]

131. Security is a key aspect of the identity cards scheme. Having your credit card stolen is different from having your identity stolen; one can be rescinded and replaced, the other cannot. Professor Martyn Thomas explained to us that:

> "If you start then tying authentication into biometrics which cannot be changed if they are compromised, then if you start getting those stolen electronically and using them for remote authentication, customer-not-present type authentication, you will

272 Royal Academy of Engineering and British Computer Society, *The Challenges of Complex IT Projects,* April 2004, p 22

273 Ev 104

274 Cabinet Office, *Person Specification IPS Chief Business Architect,* May 2006

275 Ev 118

276 Ev 114

277 Q 305

278 As above

> create a security nightmare where somebody's biometrics are no longer available to them to authenticate themselves for the rest of their lives."[279]

This difference raises the stakes, it changes the security landscape and impacts upon the risk mitigation processes.

132. As already discussed, the Home Office has emphasised that the system may not necessarily be one database (see paragraph 22). Katherine Courtney explained that it "is an assumption that there is one database. We have not predetermined the architecture of this system".[280] Nigel Seed clarified the point by saying that "If industry comes back and says one single monolithic database is the best way and it meets all the requirements then there may be one database. Equally, they could come back and say the security is increased by having partial data here and partial data elsewhere".[281] The solution proposed by industry will have to meet the requirements of the security accreditors.[282]

133. There have been numerous assertions that a single database would increase vulnerability and risk. The UK Computing Research Committee (UKCRC) said in evidence to the Home Affairs Committee, "if you create either a single card that has multi functions or a single database then you are adding to the nation's critical infrastructure unnecessarily and by doing that you are making a very large range of services, probably a growing range of services, vulnerable to a single attack".[283] Jerry Fishenden, National Technology Officer at Microsoft has also been reported as saying that "putting a comprehensive set of personal data in one place produces a honeypot effect—a highly attractive and richly rewarding target for criminals".[284]

134. Furthermore, we have received evidence that in order to decrease risk and increase security the solution should be based on systems already in use. Intellect has stated in written evidence that "It is industry's belief that the Government's proposed ID Cards Scheme should be built on technology and business processes that have been proven in existing implementations around the world."[285]

135. **We recommend that the Home Office give the security properties of the solution a very high priority, not only from the point of view of being trustworthy but also to ensure that the security features do not adversely impact upon the operation of the scheme. Furthermore, we suggest that if possible, the solution should be based on security architectures, technology and processes that are already in use.**

279 Q 489 (Thomas)

280 Q 345

281 Q 349

282 Q 351 (Bloomfield)

283 Home Affairs Select Committee, *Identity Cards*, p 22

284 Gerri Peev, "ID Cards will lead to 'massive fraud'", *The Scotsman*, 18 October 2005

285 Ev 91

7 Public engagement and communication

136. There has been criticism over the lack of public debate regarding the technologies supporting the identity cards scheme. Dr John Daugman from Cambridge University said that "public discussion of scientific issues related to biometrically-enabled ID cards has been of a poor standard".[286] Jerry Fishenden from Microsoft agreed, saying that "communication, such as it is, is both insufficient in quantity, if you like, and the quality of it at the moment is not of the calibre I would expect".[287] Dr Tony Mansfield from the National Physical Laboratory said that "given that there can be so many misconceptions about how the scheme should work, would work, there are some problems with communication".[288] Furthermore, Intellect has suggested that the debate has been skewed towards biometric technologies. It has stated that "it is important to recognise that although the ID Card debate has focused primarily on biometrics so far, there is more to ID Cards and identity management."[289]

137. The Home Office has attempted to communicate with the public. The identity cards programme, in co-operation with the UK Passport Service, has developed a public communications strategy, which has involved various activities including:

a) regional biometric roadshows in September and October 2005 where members of the public could have their iris and fingerprints recorded and verified;

b) production of customer leaflets explaining biometrics, how facial biometrics will work on the e-passport and how biometric passports will fight fraud;

c) making information regarding the scheme available on the IPS website; and

d) creation of a DVD to explain the implementation of the identity cards programme.[290]

We acknowledge the Home Office's efforts to engage the public and recommend that these efforts intensify as the scheme progresses.

138. We also note however the apparent disconnect between the Home Office's activities and the poor quality of public debate highlighted in the evidence that we have received. We believe that the problem may result from prominent media reports, for example about the Atos Origin report, the skimming of information off biometric passports, the LSE Identity Project Report and an early variant identity card. As already mentioned, the Atos Origin report was not designed as a trial to look at the performance of technology (see paragraph 88). However, following the leak of the Atos Origin report in October 2005, there were numerous articles detailing the "failures of biometric technology".[291] In February 2006,

286 Ev 83

287 Q 516

288 Q 539 (Mansfield)

289 Ev 103

290 Ev 119-120

291 Gerri Peev, "ID cards will lead to 'massive fraud'", *The Scotsman*, 18 October 2005; Tim Shipman, "The 'faulty' ID cards that could fail to identify a terror suspect", *Daily Mail*,17 October 2005, p5; Marie Woolf, "ID Card scanning system riddled with errors; Hi-Tech equipment could misidentify one in 1,000 people, say official", *Independent on Sunday,* 16 October 2005, p 10; Oonagh Blackman, "ID Cards won't work if you've got brown eyes says Govt. Minister", *The Mirror*, 17 October 2005, p 16

there were several reports explaining how a Dutch firm had skimmed data from a biometric passport.[292] As mentioned previously, the Identity Project at the London School of Economics has been the subject of numerous press reports that have emphasised its criticisms of the Home Office scheme.[293] More recently, internal e-mails from the Office of Government Commerce published in the press have referred to an early variant card, which other newspaper reports have speculated would just include a facial image or two fingerprints.[294] Such articles disseminate misleading or factually inaccurate information, which undermines public confidence in the scheme and allows misconceptions regarding the technology to develop that may cause problems later.

139. Although some of these articles contained rebuttals from Home Office officials, of course not all did so and we acknowledge that the media can be selective in choosing information. The National Physical Laboratory notes that "the media has often been selective in quoting our responses, using only those that support the thrust of their story".[295] Qinetiq has also said that "it is inevitable that the media will focus on the sensational or the worrying stories. More attention needs to be given upfront to combining a media-savvy approach with informed technical input."[296]

140. Given that the Minister, Joan Ryan, has acknowledged that "When we are running this out to the public, there is a huge issue of trust", we encourage the Home Office to engage proactively with relevant journalists.[297] The departmental Chief Scientific Adviser explained to us that he was already taking this approach in other areas such as crime. Regarding the positive presentation of science and statistics in the media, he said that:

> "There are some real difficulties there. I am not blaming the journalists or the press; I think there is a problem. There is a problem because, as we know, we do tend to have a rather weak scientific and numeracy culture in this country which does not help."[298]

We urge Professor Wiles to apply this approach to other areas of science within the Home Office, in particular the technologies supporting the identity cards scheme.

141. **We support the identity cards programme's public communications strategy. However, we believe that this effort has been undermined by damaging media reports. We recommend that the Home Office seeks to inform the identity cards debate with accurate statistics and evidence, and communicates with the media more clearly in addition to seeking to rebut allegations as they arise.**

---

292 Fran Yeoman, "Dutch firm exposes flaw in security of biometric passports", *The Times* , 3 February 2006, p 17; Allison Martin,"Chip and Pinch; ID Card fears after biometric passport 'cracked' in 2 hours", *The Mirror,* 2 February 2006, p 4

293 Jimmy Burns, "Treasury should take over project, says study", *The Financial Times,* 17 January 2006, p 2

294 "Emails from Whitehall officials in charge of ID cards", *The Sunday Times,* 9 July 2006;*Jean* Eaglesham, "ID cards procurement put on hold", *The Financial Times,* 12 July 2006, p 2

295 Ev 110

296 Ev 86

297 Q 1154

298 Q 1118, HC 900–x, (to be published in HC 900–II, Session 2005–06)

8 Conclusion

142. This inquiry has uncovered several areas in which the Home Office's treatment of scientific advice and evidence appears to be following good practice. The establishment of committees of experts, the use of OGC Gateway Reviews, discussions with international experts and the commitment to trialling technology are examples. In particular, we welcome the Home Office's assertion that it will take a cautious approach to the scheme and that implementation will be gradual. The Home Office is currently in the process of gathering evidence and advice; how it uses that information will have an impact upon the scheme.

143. There are however also several areas of the scheme that cause us great concern. Firstly, the identity cards programme team appear to have concentrated on biometrics because it is an emerging technology. This focus has seemingly detracted attention from other technological and scientific aspects of the programme. Whilst several processes for feeding in scientific advice from experts have been established for biometrics, similar processes are lacking in ICT and social science. We recognise that ICT is not the responsibility of the departmental Chief Scientific Adviser but, despite correspondence with the Home Office, we are still unclear about who actually has this responsibility within the programme. It seems that this lack of clarity might have been exacerbated by the recent creation of the Identity and Passport Service. This is undesirable, particularly in a scheme that is as reliant upon a complex and large ICT solution as the identity cards programme. Furthermore, it seems that the Home Office appears to be isolating itself from the wealth of expertise available in other departments and this may cause problems with interoperability in the future.

144. The division between biometrics and other aspects of the programme has been emphasised by an inconsistent approach to scientific advice and evidence. Whilst some aspects of the scheme, such as the types of biometrics to be used have been determined, other areas, such as the architecture of the ICT system have been left to industry. This inconsistency has caused confusion in the wider community and the extent to which the scheme will be prescriptive is not clear. Such confusion has been exacerbated by the lack of transparency of the scheme. In addition, there is a lack of clarity regarding the overall scope of the scheme, the scenarios when the card might be used, the procurement process and the OGC Gateway reviews. With regard to the procurement process, it is particularly important if the Home Office is intending to take a flexible approach to its timetable that it keep the relevant communities informed. In relation to this inquiry, greater clarity regarding the Home Office's approach to risk management, costs and systems architecture may have allayed the concerns expressed in this Report.

145. We emphasise however that the identity cards scheme has at least another two years before identity cards begin to be introduced and the scheme has still not entered the procurement phase. There is still time for the Home Office to make alterations that would improve the prospects of the project. Firstly, given that the programme is still in the pre-procurement stage we encourage the Home Office to employ a systems architect and establish an ICT assurance committee to provide advice on ICT, particularly the scheme specifications, and to review proposed solutions when that stage is reached. Secondly, we reemphasise the importance of communication with stakeholders, including scientists and

technological experts. It is crucial that the Home Office increases clarity and transparency, not only in the areas identified as problematic but across the programme. Thirdly, we reiterate that once trials commence, if the evidence gathered indicates the need for changes in the programme, such changes should be made even if the timescale of the project is extended in consequence. If appropriate changes are made, the identity cards scheme could still become an example of good practice in the handling of scientific advice, risk and evidence.

Conclusions and recommendations

Stakeholder engagement

Consultations

1. The Home Office has consulted the wider community and has tried to apply best practice in this area. However, stakeholders are not satisfied with the nature of consultation and feel that consultations have been unduly limited in scope with unclear evidence gathering objectives. As a result, the wider community does not have the level of confidence in the scheme that could be expected following a successful consultation process. (Paragraph 31)

2. We recommend that the Home Office undertakes future consultations on scientific and technical issues as well as the procurement process. (Paragraph 33)

Transparency

3. We conclude that the processes by which scientific advice is incorporated into policy are not completely transparent and that organisations are not receiving feedback regarding their advice. We urge the Home Office to fulfil their welcome commitment to make it clear how and what advice has been incorporated into the development of future policy, particularly the technical specification. (Paragraph 36)

Clarity

4. We are aware that political pressures inevitably impact on the scheme, but it is highly regrettable that the emphasis on different aspirations has changed. This has created uncertainty for the public and industry alike. We hope that the situation will stabilise now that the Bill has received Royal Assent. (Paragraph 37)

5. We urge the Home Office to finalise the scope of the scheme and the technical standards needed for interoperability as soon as possible. (Paragraph 42)

6. In order to clarify when and how the card might be used, we recommend that the Home Office releases more information regarding what personal data will be revealed in different scenarios, including in an online context. Until this information is released, it is difficult to ascertain the true scope of the scheme and to fully understand how technology will be used within the scheme. (Paragraph 45)

7. We recommend that the Home Office issues a clear timetable for the publication of the technical specifications and defines procurement processes and stages. (Paragraph 46)

8. We are disappointed that two years after the Home Affairs Committee inquiry into identity cards the problems regarding clarity have not been resolved. We urge the Home Office to address these issues immediately. (Paragraph 47)

Sources of scientific advice

Advisory committees

9. We welcome the establishment of the Biometrics Experts Group and the Biometrics Assurance Group, although we regret the time that the Home Office has taken to set them up. We support the involvement of Sir David King and believe that the Assurance Group has the potential to work well, particularly in providing consistent advice across Government. We seek confirmation from the Home Office that the Biometrics Assurance Group will be given the direction, tools and time to fulfil its tasks in practice and that the Group's recommendations will be taken into account. (Paragraph 53)

10. We recommend that the Identity and Passport Service establish an ICT Assurance Committee consisting of academics and industry experts and that this committee reviews the programme specifications relating to ICT. (Paragraph 55)

11. We welcome the work that has been undertaken over the last two years by the Government in developing the network of Chief Information Officers and more recently, Chief Technology Officers. We have not received any evidence demonstrating that these changes have impacted upon the identity cards programme. Given the central role played by ICT in the identity cards programme, we recommend that the involvement of ICT professionals within Government in the scheme be made clear and, if appropriate, that the Chief Information Officer chair the ICT Assurance Committee. (Paragraph 57)

Academia and learned societies

12. We believe that the Home Office is not taking full advantage of the impartial advice that could be offered by the academic computer science and information systems community. We recommend that the Home Office uses the ICT Assurance Committee in order to fully engage the academic ICT community. (Paragraph 61)

13. The LSE reports served a useful purpose in opening up debate on the scheme but the resulting emphasis upon the cost of the scheme and the errors in the initial interim report inhibited the development of the necessary wide-ranging debate. (Paragraph 65)

14. We are disappointed by the nature of the Government's reaction to the criticisms outlined in the LSE reports. We believe that the way in which the LSE reports have polarised the debate regarding identity cards, whether intentionally or not, has been detrimental. The Home Office would have been better advised to put together a dispassionate critique of the LSE Identity Project Report rather than seek to undermine its credibility and motivation. (Paragraph 67)

Industry

15. We recommend that, particularly as it enters the procurement phase, the Home Office works to develop further its relationships with industry. Industry is a

significant source of scientific and risk reduction advice as well as being a pool of potential suppliers. We reiterate that the Home Office needs to engage in wide-ranging debate with industrial experts regarding scientific and technical aspects of the scheme. (Paragraph 70)

Co-ordination within Government

16. We recommend that the Home Office undertakes a cross-Government consultation regarding its plans for technology to support the identity card scheme before the specifications of the scheme are finalised and that it makes the findings of this consultation public. (Paragraph 76)

International models

17. We recommend that the Home Office continues to develop international links during the programme but stress that the limitations of advice and evidence from other schemes must be recognised by Ministers in the light of the unprecedented scale, the use of multiple biometrics and the complex IT requirements of the UK scheme. (Paragraph 80)

18. In order to build public confidence in the technologies involved, we recommend that the Home Office publishes an overview of the scientific advice and evidence that it receives as a result of international co-operation. (Paragraph 81)

The evidence base

Trials

19. We welcome the Home Office's commitment to publicising fully its plans for trialling once the procurement process has begun. In order to continue this move towards transparency and to build public confidence in the scheme, we recommend that the Home Office also makes public the results of these trials. (Paragraph 83)

20. We welcome the Home Office's cautious incremental approach and we encourage the Home Office, if necessary, to extend the procurement phase to ensure that enough time is taken to gather the necessary scientific evidence and to undertake all the appropriate trials. In view of the potential adverse impact on large numbers of people, it is better that the scheme is late and workable than on time but flawed. (Paragraph 84)

21. We recommend that the Home Office publicly outlines the ways in which the results of the trials have influenced and changed the programme. (Paragraph 85)

22. We seek assurance that the Home Office will not limit the number, scope or quality of technology trials in order to stay within the allocated budget. We recommend that the Home Office ensures that sufficient funding is available to undertake the necessary technology trials for this scheme and that it retains flexibility regarding the trials that may be required. (Paragraph 86)

23. There is evidence that whilst trial plans were set out clearly the processes with which they were enacted lacked rigor. As a result, the Home Office has selectively used evidence from the biometrics enrolment trial to support its assertions. We believe that the Home Office has been inconsistent regarding the status of this trial and this has caused confusion in relation to the significance of the evidence gathered about biometric technologies. We recommend that the Home Office clarifies whether or not it accepts the validity of the results gained during the trial regarding the performance of biometric technologies. (Paragraph 88)

24. Given the findings of the biometrics enrolment report regarding the performance of current biometric systems, we seek reassurance from the Home Office that systems will be adapted as necessary to improve performance levels and that final performance levels will be verified by independent testing. (Paragraph 89)

25. We note the lack of independent evidence relating to the performance of iris scanning and welcome the Home Office's commitment to undertake a large-scale matching test using pre-recorded biometrics. Given the relative lack of information available publicly regarding the performance of biometrics in a national scheme, we recommend that once the scheme is established the Home Office publishes details of the performance levels of the technology. (Paragraph 91)

26. We are surprised and concerned that the Home Office has already chosen the biometrics that it intends to use before finishing the process of gathering evidence. Given that the Identity Cards Act does not specify the biometrics to be used, we encourage the Home Office to be flexible about biometrics and to act on evidence rather than preference. We seek assurance that if there is no evidence that any particular biometric technology will enhance the overall performance of the system it will not be used. (Paragraph 93)

27. We note the lack of explicit commitment from the Home Office to trialling the ICT solution and strongly recommend that it take advice from the ICT Assurance Committee on trialling. We seek an assurance that time pressure and political demands will not make the Home Office forgo a trial period or change the purpose of the scheme. (Paragraph 95)

Research and development

28. We recommend that the Home Office identifies the gaps in the evidence base underpinning the identity cards programme, that it commissions research to fill these gaps and that it feeds any new developments into the scheme where appropriate. This process should be overseen by the departmental Chief Scientific Adviser. (Paragraph 96)

29. The Home Office cannot afford to delegate responsibility for horizon scanning to others. We recommend that the Home Office actively undertakes horizon scanning activities relevant to the technologies involved in the identity cards programme and that it develops mechanisms to feed this information back into the scheme. (Paragraph 97)

30. We urge the Home Office to commission, and where appropriate fund, research focused on the specific requirements of the information technology systems in the identity cards scheme rather than relying on general existing study results. (Paragraph 98)

Technology and operating costs

31. We recommend that the identity cards programme team returns to the KPMG audit report and implements its recommendations. Furthermore, we re-emphasise that the Home Office needs to work out how costs will impact on performance and we seek reassurance from Government that cost limitations will not compromise the level of performance that is accepted. (Paragraph 102)

32. We are sceptical about the validity of costs produced at this early stage. We acknowledge that the release of firm overall costing has been driven by political imperatives but the Home Office could have credibly given a broad range instead of precise figures. We note the danger that a desire to keep below a costs ceiling might drive the choice of technology. We seek assurances that the costings are flexible. We strongly recommend that, once the procurement process has taken place, the Home Office publishes a breakdown of technology costs, including set-up costs, running costs and predicted savings as a result of the scheme in the Home Office and elsewhere. (Paragraph 105)

33. We recommend that the Home Office prioritise funding as necessary to ensure that required social science research is undertaken and if necessary commissioned. In particular, we emphasise the need to undertake work to understand the attitudes of prime users towards the current proposals. (Paragraph 109)

34. We recommend that the Home Office establishes a clear process by which advice from external social science experts regarding future research and the social science aspects of the programme can feed into the scheme. Once research has been undertaken, we urge the Home Office to develop the expertise that will allow it to follow up the results. (Paragraph 111)

The treatment of risk

Treatment of risk

35. The Home Office has provided us with details of the risk management strategy within the identity cards programme. However we are disappointed that the Chairman was not allowed to view the risk register in confidence. In the light of the evidence provided to us, we are somewhat reassured by the Home Office's risk management strategy. Any delay to the procurement process will postpone the treatment of various risks. We seek assurance that the timing of the procurement process will be considered in relation to risk management. (Paragraph 116)

36. We recommend that the Home Office make details of its risk model public and that it takes steps to ensure that advice regarding risk management can feed into that model. (Paragraph 117)

37. We recommend that an overall indication of the outcomes of the OGC Gateway Reviews, but no specifics, be made public in order to increase confidence in the scheme. (Paragraph 119)

38. It is important that the impact of a politically-imposed deadline will not override the impact of scientific advice or evidence on the readiness of the scheme and we seek reassurance from the Government on this point. (Paragraph 120)

39. We emphasise the importance of the development of an holistic approach to risk management in order to ensure that focus on biometrics as an emerging technology does not detract attention from other aspects of the scheme. (Paragraph 122)

ICT system

40. Industry is hoping that the commencement of procurement and the release of specifications will clarify the Home Office's position. Once the specifications have been released, we urge the Home Office to take steps to ensure that the specifications, requirements and risks have been clearly understood by all involved. (Paragraph 126)

41. The Home Office is reliant on external expertise in the area of ICT and is unable to act as an intelligent customer of scientific advice. We recommend that the Home Office uses a senior and experienced systems architect to advise on the specifications and to provide support during the procurement process. (Paragraph 129)

42. We recommend that the Home Office give the security properties of the solution a very high priority, not only from the point of view of being trustworthy but also to ensure that the security features do not adversely impact upon the operation of the scheme. Furthermore, we suggest that if possible, the solution should be based on security architectures, technology and processes that are already in use.(Paragraph 135)

Public engagement and communication

43. We support the identity cards programme's public communications strategy. However, we believe that this effort has been undermined by damaging media reports. We recommend that the Home Office seeks to inform the identity cards debate with accurate statistics and evidence, and communicates with the media more clearly in addition to seeking to rebut allegations as they arise. (Paragraph 141)

Formal minutes

Thursday 20 July 2006

Members present:

Mr Phil Willis, in the Chair

Mr Adam Afriyie	Mr Brooks Newmark
Mr Robert Flello	Bob Spink
Dr Evan Harris	

Draft Report, Identity Card Technologies: Scientific Advice, Risk and Evidence, proposed by the Chairman, brought up and read.

Ordered, That the Chairman's draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 145 read and agreed to.

Resolved, That the Report be the Sixth Report of the Committee to the House.

Ordered, That the Appendices to the Minutes of Evidence taken before the Committee be reported to the House.

Ordered, That the Chairman do make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Wednesday 18 October at nine o'clock.

Witnesses

Written evidence

Reports from the Science and Technology Committee

Session 2005-06

First Report	Meeting UK Energy and Climate Needs: The Role of Carbon Capture and Storage	HC 578-I
Second Report	Strategic Science Provision in English Universities: A Follow–up	HC 1011
Third Report	Research Council Support for Knowledge Transfer	HC 995-I
Fourth Report	Watching the Directives: Scientific Advice on the EU Physical Agents (Electromagnetic Fields) Directive	HC 1030
Fifth Report	Drug classification: making a hash of it?	HC 1031
First Special Report	Forensic Science on Trial: Government Response to the Committee's Seventh Report of Session 2004-05	HC 427
Second Special Report	Strategic Science Provision in English Universities: Government Response to the Committee's Eighth Report of Session 2004-05	HC 428
Third Special Report	Meeting UK Energy and Climate Needs: The Role of Carbon Capture and Storage: Government Response to the Committee's First Report of Session 2005-06	HC 1036
Fourth Special Report	Strategic Science Provision in English Universities: A Follow–up: Government Response to the Committee's Second Report of Session 2005-06	HC 1382

Oral evidence

Taken before the Science and Technology Committee

on Wednesday 22 March 2006

Members present:

Mr Phil Willis, in the Chair

Adam Afriyie
Mr Jim Devine
Mr Robert Flello
Dr Brian Iddon
Margaret Moran
Bob Spink
Dr Desmond Turner

Witnesses: **Ms Katherine Courtney,** Director, **Dr Henry Bloomfield,** Technical Lead, Identity Cards Programme, **Mr Nigel Seed,** Project Director, National Identity Register and Operational Technology Infrastructure, and **Mr Marek Rejman-Greene,** Head of Biometrics Centre of Expertise, Home Office, gave evidence.

Q262 Chairman: May I welcome our witnesses and members of the public to the first public session in terms of our case study on technology supporting identity cards within our broader inquiry of looking at scientific advice to Government. I emphasise that we are looking at the issues of process today rather than trying to decide or best guess which technology is best for the purpose for which the Government has identified this scheme. I start by asking Ms Courtney if you could introduce yourself and indeed the rest of your panel briefly to us.
Ms Courtney: I am Katherine Courtney. I am the Director of the Identity Cards Programme. As a brief introduction, I was appointed to this post in September 2003 as the Programme Director. My background is in the private sector, principally in the telecoms industry. I would like to introduce Dr Henry Bloomfield from my team. He joined the programme in October 2003 as one of the technical leads on the team. His background is really technical project management from the finance industry. Nigel Seed is our major project director, leading on the development of the National Identity Register and the technology infrastructure for the programme. He joined the programme quite recently, in November last year, from the MoD where he was project managing the AWACS Mission System mid-life update programme. Marek Rejman-Greene is the senior biometric adviser at the Biometrics Centre of the Home Office. Last year, the Home Office set up a centre of expertise under the leadership of the Chief Scientific Adviser, Paul Wiles. Marek joined us from BT in the summer of last year.

Q263 Chairman: Thank you. The technology that will be used by the scheme depends on its aims and uses. What do you understand those aims and uses to be?
Ms Courtney: The aims of the scheme I think are laid out quite clearly on the face of the legislation that we are taking through the parliamentary process at the moment. They are to combat illegal immigration and illegal working; to provide a secure and convenient form of verification of identity for individuals accessing services; to provide additional tools in the armoury for combating serious crime and countering terrorism; and to attempt to reduce the growing problem of identity fraud that we face in the economy today.

Q264 Chairman: Has that grown since the original concept by David Blunkett four years ago and is it likely to grow again?
Ms Courtney: I do not believe it has grown. If you look back to the original consultation at the time of what was called an entitlement card scheme, it did include similar aims and objectives. Obviously, we have since refined and clarified them to be more specific. In responding to feedback on the consultation and on the scrutiny of the draft legislation, we have, for instance, stated the aims of the statutory purposes quite clearly on the face of the Bill in order to attempt to make sure that we have the scope of the scheme quite clearly defined.

Q265 Chairman: In terms of managing this project, you are absolutely clear what it is aiming to do, what its purposes will be, and you will build the technology around that?
Ms Courtney: Yes, the technology is an enabler to achieving this objective.

Q266 Bob Spink: There is a perception in the House of Commons, and indeed in the public, that the emphasis has certainly changed if the parameters have not. Certainly the emphasis between them has changed dramatically over the last years and months. Is this your perception?
Ms Courtney: No, it is not my perception. I am not sure what the change of emphasis you are referring to is, so it is difficult for me to respond.

Q267 Bob Spink: It is moving away from "this will tackle terrorism" to "this will help us to tackle illegal immigration, benefit fraud and ID fraud".

Ms Courtney: I think the original consultation around the principles was triggered by a Cabinet study into identity fraud, and so one of the clear aims of the scheme has always been to tackle identity fraud. As the original consultation was, as I said, called an entitlement scheme, the focus there was also really about accessing services and making sure that people who did not have rights to free service were not abusing the system and defrauding the system. I do not see that the emphasis has changed.

Q268 Bob Spink: It must be that the public, we in the House of Commons and the media have got it wrong then? Thank you.
Ms Courtney: I never said that.

Q269 Chairman: Please feel free to bring in your colleagues when it is appropriate. We have received written evidence that the technological architecture of the scheme is very much dependent on the business case being made. Would you agree that they are interdependent on each other? Are the business requirements set?
Ms Courtney: The business objectives and the functional requirements of the scheme are set, but I should say that they are set in two regards: firstly, because we are building on a series of developments that are taking place incrementally through the Passport Service, Immigration Nationality Directorate, UKVisas, et cetera, and so we know that there are certain business processes and technological requirements that are givens in how we operate this scheme. They are also set because in order to undertake a business case evaluation, we have had to define a reference solution for ourselves, otherwise we would not be able to have any sort of cost assumptions built into the business case.

Q270 Chairman: Is all that being done in-house?
Ms Courtney: Not solely in-house, no; in terms of the reference solution, we have consulted quite widely with experts. We have also done quite a lot of market sounding and engagement through seminars and workshops and one-to-one dialogue with the industry to inform our thinking on that. I would like to stress that it is not about setting the technological architecture because we intend to take this, subject to parliamentary approval, to a competitive procurement process and intend, according to best practice, to focus on the outcomes we are trying to achieve and not dictate to the industry what the technical architecture should be.

Q271 Chairman: We will come back to the procurement process. Clearly there are many experts who say, and I do not just mean parliamentarians who always have a vested interest, that this is not a feasible project, it is not do-able. What evidence do you have which says that you can actually do it? Where is that evidence?
Ms Courtney: We have been looking at this for many years, actually several years before I joined the programme as a matter of fact. Before the policy decisions in principle were even taken, quite a lot of feasibility analysis went forward. In parallel with the consultation on the principles of the scheme, the Passport Service at that time also commissioned a feasibility study from the National Physical Laboratory into the proposed technologies, so there were feasibility studies done around in particular two of the key technologies: the biometric technologies and the smartcard technologies. Those studies came back showing that the technical risks to a programme like this were medium risks and were manageable and actually the important thing to focus on was of course the business risks and making sure that we are getting the business process right and all the other factors around how you identify a person and register their identity, and then confirm it.

Q272 Chairman: I find that answer, with the greatest respect, absolutely astounding. Two weeks ago, the Committee was in the United States talking to the Department of Homeland Security who said exactly the opposite to what you have said. They said that in terms of their starting to go out to procurement on their major project involving biometrics for ID cards, the technology was not there and that they were not in a position even to recommend to the administration that a procurement process should start, and yet you say that you have done the feasibility and you are confident that it can be done. What more do we know? They are paranoid about security in the States at the moment.
Ms Courtney: We do engage with the Department of Homeland Security. I cannot comment on what they may have told you in a meeting. We have done quite a lot of looking at programmes in other countries that are using biometric technologies quite successfully. From our own operational experience at the Home Office, as you will know, we have quite a successful asylum registration scheme which uses biometric technologies. We have been running very successful pilots on the biometric visa programme. We have had good success with our project IRIS as well through the eBorders programme and the Passport Service has also experienced some very good success with the facial biometrics it has already implemented.

Q273 Chairman: We will return to that later because some members of the Committee are particularly interested in following up some of those technologies. Let us say that the Bill gets through Parliament and receives the Royal Assent fairly quickly, the programme is likely to enter the procurement process very soon. Have you set a statement of technology requirements for the procurement process?
Ms Courtney: We have and, if you would like to explore our plans in that area in more detail, I could ask Nigel Seed to talk to this.
Mr Seed: We have what we are calling level one requirements which describe not in very detailed terms what we want the programme to do. That will go out initially to all the companies that have expressed an interest. They will come back and tell us what their proposals are. We will then down-select to a smaller group that will receive the more

detailed requirements, all of which, as Katherine says, will be in output based terms. We will not be specifying technologies. We will be telling them what the system has to do and then the leaders in the field that we already know are interested in the project will come back and propose ways of doing it. From there we will go forward and physically test their proposals to make sure that they are going to work and we are not buying a pig in a poke. We will put live people through the system, move the data about, and do the matching technologies before we go forward to contract.

Q274 Chairman: When you are talking about feasibility studies, that has nothing to do with actually seeing whether certain technologies or a mixture of technologies are feasible in terms of the project and its aims?
Ms Courtney: We have done feasibility studies into that. Perhaps it would be useful to expand a little bit on what the original NPL study focused on and also our future programmes in that area.
Dr Bloomfield: The NPL study, which was conducted during 2002 and reported in the early part of 2003, was initiated by a request to find out what the possibility was of using biometrics in the entitlement card scheme. That looked at the capabilities of various biometric technologies and came up with conclusions, for example with fingerprints, whether one should use pattern-based techniques or minutiae-based techniques; how many fingerprints should be used for a population the size of the UK, and so on. These recommendations were in the final version of the report, which was then published. Many of those recommendations have made their way through to our requirements to date.

Q275 Chairman: In terms of the feasibility study, it is stated on page 3 that the practicalities of deploying either IRIS or fingerprint recognition in such a scheme are far from straightforward. Your feasibility study said that it was not straightforward and it was not something which you had a handle on.
Dr Bloomfield: I think that is absolutely right. There are lessons that the deployment of these technologies is far from straightforward. Those are the kinds of things we wanted to learn from the feasibility study. It was that sort of conclusion from that feasibility study that led to the design of the later UKPS biometric enrolment trial, which specifically looked at the process and people issues, which are key to the successful deployment of biometrics.

Q276 Chairman: But, Henry, you are moving to this phase one procurement process and it is going to be therefore led by the industry. You do not know quite what you want or what the industry might come up with. You said that, Nigel.
Mr Seed: It is not a case of our not knowing what we want. We are not telling them how to implement what we want. It is slightly different. We are not the experts in the technology; they are. If we were to tell them to select a particular piece of kit, we could be making a bad choice.

Q277 Chairman: Will there be transparency about this process?
Ms Courtney: Yes.

Q278 Dr Iddon: I want to explore where you are getting your evidence on biometrics from. I notice that there have been set up two groups: one, the Biometrics Experts Group, which I understand is a Home Office-originated group with advisers external to the Department; and another the Biometrics Assurance Group, which I understand is run by the Chief Scientific Adviser, with academics and industrialists as part of it.
Ms Courtney: Yes.

Q279 Dr Iddon: I was wondering why we set up those two groups; which one was set up first; why we need two groups; and why they have not collided.
Ms Courtney: We not only have our own internal biometrics experts advising us but we also wanted to set up that wider community of biometric experts. We can talk a bit more about how that group operates, but we use the Biometrics Experts Group in reviewing our own plans, our own understanding, of what the technical risks are and how we can work with the technologies, and also to do that horizon scanning around what is likely to be developing over time. We then also felt, and I felt quite strongly as Programme Director, that we needed independent assurance of the advice that we were receiving. So we asked Sir David King if he would chair an independent panel of experts in the field who could review the advice that we were receiving and the decisions that we were taking and provide a quality assurance from an independent perspective about that advice and about the decisions that we were taking as a result. I am quite happy to speak in more detail about either of those groups but they serve two very different purposes.

Q280 Dr Iddon: There is no cross-contamination between the experts on one group and the experts on your group?
Ms Courtney: No, certainly obviously the experts who work in my team do have to present our materials to the assurance group, so that they are kept sighted on what we are doing and are able to provide the assurance function for us, but the Biometrics Assurance Group will be publishing a report of its reviews of the work that we are doing and that is really for Sir David King. It is not that we are in any way directing the assurance group.

Q281 Dr Iddon: Which of these groups started first?
Ms Courtney: We put our internal advisers together obviously over a period of time, but from the very beginning we had expert advisers working on advising us about the practicalities. The assurance group was convened for the first time last year, I believe, once we had got to the point where we had sufficient detail in our plans and assumptions that we could put it in front of the body and have it reviewed.

Q282 Dr Iddon: If I can get the roles correct and simplified, you have a group looking at biometrics and the Chief Scientific Adviser has another group that is looking at the evidence that you are presenting to the Government to make sure that that is sound evidence. Do I understand that correctly?
Ms Courtney: Yes.
Dr Bloomfield: The Biometrics Experts Group is very much a doing group (it is very much involved in the formation of our requirements and our testing strategies, and so on) whereas the assurance group is what it says; it does assurance on our biometric requirements. The intention is that it should also act as an assurance group for other biometric schemes throughout government.

Q283 Dr Iddon: They are both government groups, of course. Who decided to select the members of each group and on what basis?
Ms Courtney: Perhaps I could ask Marek to speak to that.
Mr Rejman-Greene: With regard to the Biometric Assurance Group, it was felt that because of the complexities, as we have referred to that, about technologies and the way in which the reports of the feasibility study work is so tentative, it needed to have external experts. The problem is in the biometrics field there are relatively small numbers of experts who are not committed to either programmes such as the ID cards or related programmes within the Home Office. A number of ways of looking at the membership of that assurance group were tried out, one of which was to look at the various aspects to do with the use of biometrics: is it the technology itself; the usability; the perceptions about it; the application of the technology? We tried to look and see if we could fit in the people who are independent and world-wide experts in each of those areas and select them and invite them to join the group. Obviously not everyone we invited joined that group. The Experts Group, on the other hand, is very much a group that helps internally the development of the programme, the development of the testing schedules and the procurement requirements. It is very much internally focused in supporting the ID cards Programme itself. The other point about the assurance group is that it does not just necessarily look at the ID Cards Programme; it will also look in the future at all the other related programmes using biometrics, such as the UK Visas Programme, programmes to do with immigration and eBorders.

Q284 Dr Iddon: Before these groups were set up, where were you obtaining your evidence from?
Mr Rejman-Greene: There was a continuous process of working with consultants, specialists and biometric experts. Perhaps you would like the names of the people in those programmes. There were: Professor Jim Wayman from San Jose State University, Tony Mansfield from the National Physical Laboratory, Philip Statham from CESG. Those people were continuously being involved in the discussions about the development of the programme and its feasibility.

Q285 Dr Iddon: My problem is, and you said it just a moment ago, that biometrics is such a small field that I cannot understand how these two groups can become so independent that the assurance group can correctly analyse, quantify and assure the other group that what is happening is correct.
Mr Rejman-Greene: The assurance group members are not involved in any way, shape or form with the programme itself.

Q286 Chairman: Again, I find that quite staggering because one member of your assurance group, Dr John Daugman, in fact has the world-wide rights to iris scanning. He is the guy that has all the patents. How can you possibly have him on an independent assurance group looking at iris technology when he owns it all?
Mr Rejman-Greene: I will respond to that. First of all, the key patent about the use of iris recognition is now open.

Q287 Chairman: Not quite yet.
Mr Rejman-Greene: It is very close to that. Therefore, alternative methods of using that approach have been developed and are being researched as we speak now and commercialised. He does not own it but a company in the United States that actually owns those patents.

Q288 Chairman: But he spends all his time actually rubbishing anyone who attacks iris technology.
Ms Courtney: I would like to add that the Chief Scientific Adviser at the Home Office was involved in identifying appropriate assurance group members and reviewing their CVs and their global status, and the members of the assurance group are all independent, very well respected academics, who fiercely guard their independence.

Q289 Chairman: And their commercial powers.
Ms Courtney: We have every confidence that the assurance group is able to provide the level of independent view in countering the experts' advice that we pay for, if you see what I mean.

Q290 Adam Afriyie: You did not directly answer the question as to who appointed the members of this panel.
Ms Courtney: I believe officially they are appointed by Sir David King as the Chairman of the panel[1].

Q291 Dr Turner: Ms Courtney, it is our understanding that what you are setting out to do is an extreme challenge, technologically speaking, and that the fused combination of the three biometrics in one system and a massive system database which is going to grow to about 50 million individuals is something that has never even been done. Why, at the start, have you chosen these particular three biometrics?

[1] *Note by the witness:* Sir David King chairs the Biometrics Assurance Group, but the Home Office appoints the independent industry figures and academics who make up the group.

Ms Courtney: When we reviewed all the literature, the research, also the practical experience from programmes around the world, we looked at systems that did use more than one biometric, which is now increasing. Obviously you will know, for instance, that the International Civil Aviation Organization has begun with the facial biometric and is adding fingerprint biometric to that as part of its common standards. On residents permits, there is an EU Directive that we are seeking to comply with which also requires both facial biometric and fingerprint biometric, et cetera. We have looked at those. We have looked for the most mature biometric technologies, which happen to be the face, iris and fingerprints. We have looked at the ones also that provided the best operational performance on a value-for-money basis. The field is evolving all the time. I think one of the challenges has to be to design a system that is flexible enough possibly to accommodate advances in the technology later down the line.

Q292 Dr Turner: What evidence do you have that this combination will actually work, given even that your own 2003 feasibility report found that facial recognition was not a feasible proposition? You are going to put that in association with two other biometrics to compound the difficulties. Obviously, the machines for reading fingerprints, iris, et cetera, are quite different. It would be very difficult to make one portable machine to measure all three biometrics. What evidence do you have that it will actually work in practice, given that working means in practice that you are going to need something which has a very, very low error rate, otherwise the case that would occur at airports and so on is just unimaginable?
Ms Courtney: I think there is often a misunderstanding about the function of the biometrics as part of the system. The function for us of the multiple biometrics, and again we have always said that this is something that we have been in consultation with the industry about, needs to be tested during the procurement process in order to ensure that we have gathered the evidence base, that those biometrics will enhance the performance of the system. There has been a recommendation that we have been given that no single biometric is the solution. What we are looking for from the multiple biometrics is a system combined with the checking of people's biographical footprints, an interview as we are beginning now to introduce for the passport issuing process, and a number of other counter-fraud measures and, combined with all of those a system that allows us to attempt to avoid a duplicate registration of identities. The function of the multiple biometrics is part of the whole business process to try to make sure that there is a unique identity registered in the system for each person. The error rates on verification of that biometric identity are very different. In those cases what we are looking at is using the biometric in a one-to-one match—me against my details. For all of those biometrics actually the performance in a one-to-one match is fairly high. In different business applications, a different biometric might be more appropriate than others. You see, for instance, iris being used quite successfully where you have a high volume of people passing through a system, such as the expedited gate clearing at the airports. This is being used quite successfully in different countries. Fingerprints are also very successful in one-to-one matching and one-to-many matching applications as well. I think where people have a misconception is that the intent is to use all three of those biometrics in a confirmation of identity one-to-one check, and it is certainly not any of the design assumptions that we have ever made.

Q293 Dr Turner: In that case, why are you so insistent on having the three biometrics fused in one system if you say that on any one occasion you are only likely to use one of them? You have spoken about feasibility studies. Given this has not been ever achieved technically anyway, how have you been able to carry out a feasibility study to see whether the multi-modal system will work in practice?
Ms Courtney: I will ask Dr Bloomfield to say what modelling has been done on that because certainly that has been assessed.

Q294 Chairman: Could you tell us who has done that because we cannot find any evidence of that?
Ms Courtney: I will ask Dr Bloomfield to speak to that. One of the key principles that I think we need to be clear about is that this scheme needs to be accessible to the whole resident population. The policy is that anybody who is residing here for longer than three months, over the age of 16, should be able to register with the scheme. There is no single biometric today that is universally applicable to everybody. You may have individuals, for instance, who have lost their hands and are unable to register fingerprint biometrics but would be able to register a face and irises. We were looking to create a scheme that was universally accessible for people, and that was one of the important reasons.
Dr Bloomfield: I think terms such as "multi-modal biometrics" and "fusion of biometrics" have a variety of meanings. At their most extreme, "multi-modal biometrics" would imply that you are in some way taking, for example, fingerprint and iris biometrics and they are both being put into some clever algorithm, which comes up with a result. A very loose use of the term "multi-modal biometrics" would just mean that you are using both and that for those people who are, for one reason, unable to enrol fingerprints, you have an iris biometric as a fall-back. We are very much at that end of the spectrum in our thinking around multi-modal biometrics.

Q295 Dr Turner: You do not really need to use it in the way in which you have set out?
Dr Bloomfield: We are not intending that these biometrics should be used in a way where the biometric data from iris and fingerprints are in some way combined and used together in the same algorithm. What we may do is use fingerprint and iris biometrics in conjunction so that if it turns out

that your fingerprint matched against a few other people's fingerprints in the database, it is possible that an iris biometric may then be used to discriminate amongst those people.

Q296 Dr Turner: To simplify this, you are saying that if your fingerprint raises a doubt, then you turn to the iris and see whether you can resolve it that way, and then maybe go to the face if you are still stuck?
Dr Bloomfield: I am not saying that that is what we are going to do, but that is an example of how you might use biometrics in conjunction, a fairly simply method.
Ms Courtney: These are the sorts of solutions that the industry has been proposing.

Q297 Dr Turner: It sounds as if you are laying preparations for the up-front multi-modal fused system not to actually work as such?
Ms Courtney: We have never said "fused system", I should say. It has always been an intention to have a number of biometrics that we can use.
Dr Bloomfield: There are two key reasons for having multiple biometrics. One is for resolving doubts when one biometric matches; another is to ensure that as high a proportion of the population as possible is able to enrol. If people who for one reason or another have missing or damaged fingers, we would like them also to be able to enrol with iris. If you include more biometrics, then you have more likelihood of people being able to enrol. A further reason is for standards compliance. That is a very good reason for including the face biometric. You rightly said that facial biometrics do not have the same resolving power as fingerprint or iris biometrics. They are very good on one-to-one matching and if you are matching a photograph of yourself against your previously enrolled facial biometric, the performance is quite good. They are also quite good on checking someone against a fairly small watch list, but not against a large population size.

Q298 Adam Afriyie: You were showing some confidence in the match rates but the false non-match rate for fingerprints is 1 in 100; the false non-match rate for facial recognition was 1 in 10; and the false non-match rate for iris recognition was 1 in 100.
Ms Courtney: Are you quoting from our enrolment pilot?

Q299 Adam Afriyie: Yes, the false non-match rates from your own pilots.
Ms Courtney: I think it is important to reiterate that the enrolment trial was a trial of process and customer experience. It was not designed as a trial to look at performance of the technology *per se*. The NPL study recommended that we run such a pilot to look at all the business process issues around how you would register multiple biometrics for a representative sample of the population. We will be running, during the course of the procurement, again subject to parliamentary approval, operational testing of the technical systems to be able to evaluate what the actual live performance is.

Q300 Adam Afriyie: At the moment it is speculative, do you need to do further work before these numbers and statistics are clarified?
Ms Courtney: We have always said that we would do that testing as part of the procurement.

Q301 Adam Afriyie: We have had chip and pin, multi-modal biometrics (face/iris/fingerprints), testing systems, enrolment systems and verification checks. These are all to do with technology. What are the known limitations in the proposed scheme and how are you looking to address them?
Ms Courtney: Known limitations in respect of?

Q302 Adam Afriyie: In respect of the technologies that you are proposing at the moment or the route that you are taking—the plan that you have; there must be some known limitations with the technology and known limitations with the schemes with the tests that have been undertaken. What are they?
Ms Courtney: In terms of our delivery risks, which includes obviously any technical implementation risks but also it is quite importantly focused on how we organise the services, how we design the business processes, how we operate them in practice, I think Dr Bloomfield has spoken about the universality of some biometrics. We know that there are limitations. You cannot record someone's fingerprints if they do not have any fingers. That is a known limitation and one of the reasons behind our intention to use multiple biometrics to try to overcome that limitation. The biggest risk obviously in any business process is that you do not train your people appropriately. Because we are implementing this with the intention of creating an organisation based on the Passport Service, building from the good operational track record of the Passport Service in recent years, we have every confidence that we will be able to have the right training in place for people so that we can overcome that possible limitation.

Q303 Adam Afriyie: In your evidence you acknowledge that the field is fast-moving. Have you made any projections about how technology will change over the next several years during the testing and deployment of the project? If so, what are the changes that you envisage? Have you planned to incorporate them into the scheme that you are putting forward at the moment?
Ms Courtney: I might ask Marek to speak a bit about how the biometrics field is moving forward and also Nigel afterwards to say a few words about how we are building that sort of flexibility into our requirements.
Mr Rejman-Greene: You made a good point there inasmuch as the results certainly of the feasibility study in 2002. The experience in the United States with the US visa programme was based on technology which is now quite a few years old. We know, for example in the United Arab Emirates,

that there is now a programme using IRIS for nearly one million people. There is beginning to be not only an advance in the technology—the matching and the actual sensors that are picking up the fingerprints and the iris patterns in better and more inclusive ways and more and more people are being enrolled and some limitations are being countered—but the experience in terms of the larger programmes abroad is also bringing in knowledge. The future developments that we are foreseeing, certainly in terms of multimodal fusion which you mentioned, means that there is a lot of research work going on there. During the course of the deployment and early years of the programme, we would certainly ensure and ask the consortium that was winning the project to take advantage of that knowledge and home in on it.

Q304 Adam Afriyie: It certainly sounds as though the project you are proposing means that we are going to be the pioneers; we are going to be at the leading or cutting edge rather than adopting systems which are fully tried and tested in the way they are going to be used.
Mr Rejman-Greene: We are co-ordinating all those technologies, yes, but individually all those technologies are being used and being developed in single trials. I think the idea about actually working through multiple technologies is perhaps the novel element in this area in order, as Katherine said, to ensure that the highest proportion of people are "enrollable" in the system.

Q305 Dr Turner: What about the security of the system? What steps will you be taking to guard against falsification of biometrics, and perhaps the most extreme case one could imagine is that al-Quaeda would become very sophisticated and hack into your database and plant completely false biometrics for a different individual. What steps are you taking to ensure the security of the system?
Ms Courtney: From the beginning when I joined this programme, I was intent on having the best security advice possible, and so we brought in not only the government security advisers but also other independent security advisers to work with us on this. Before we had a reference solution, when we were just thinking about the principles of the scheme and the policy decisions around that, we had security advisers alongside us looking at all the possible risks of the scheme. We have had that built into our design from the beginning. We asked a long time ago for this whole scheme to be certified as part of the critical national infrastructure. It does not exist yet, but already it is listed as part of our critical national infrastructure and so it is being accredited by the government's security advisers, security accreditors, from its earliest inception.

Q306 Dr Turner: What does accreditors actually mean?
Ms Courtney: If you would like a practical example of that—

Q307 Dr Turner: Is it a kind of kite mark?
Ms Courtney: It is a bit more in depth than that. Perhaps I can ask Nigel to talk about the security accreditation.

Q308 Chairman: Can I ask you not to because we will come back to database security later. I know my colleagues are keen to do that. Before we move off this section, can I summarise where we are here? The Government has clear aims in terms of what it wants biometrics to do in this programme. You do not know, however, what the technology is because some of it may not even be there yet; it might evolve over the coming months, and so your specification in terms of level one procurement is crucial in terms of setting up parameters for what the technology, when it exists, will deliver. Am I right? Is that fair?
Ms Courtney: Yes.

Q309 Chairman: Could you either now or in writing tell us the accuracy levels that you want for each part of the biometrics? I understand not many people do not have hands. We are talking about accuracy levels for, say, somebody who is a builder and has a cut on his finger, or something of that nature. Do you have those figures now?
Ms Courtney: I would like to offer to write to you on that subject.

Q310 Chairman: If, during the process, you find that blips come into the system, are you prepared to say, "We are going to have to stop this and elongate the time in which we can deliver"? Is that part and parcel of your thinking?
Ms Courtney: Our plans have always been to take an incremental implementation to this in a step-by-step way, building on other developments and rolling out over a period of time, I think from the very first policy announcement when the Home Secretary was quite clear that there would be no big bang implementation of this scheme. That gives us lots of opportunity to test and ensure that we are getting things right. We are also taking the whole programme obviously through the Office of Government Commerce gateway process for every key component of the programme. We are also running our own internal health checks. We will not proceed to the next phase of any aspect of the programme without a clear health check that tells us that we are ready to proceed to the next stage.

Q311 Chairman: Is there evidence to show that this is the best way of developing this scheme? Is that evidence you have from elsewhere where systems have been rushed?
Ms Courtney: There is lots of evidence from the National Audit Office and the Office of Government Commerce and elsewhere. We have certainly learnt lessons from other programmes around the world.

Q312 Bob Spink: Could you tell us how many people eventually will be using this scheme or enrolled on the scheme in total, how many millions, and how

many points of access to the scheme checking people there will be eventually—how many tens of thousands of those?
Ms Courtney: The expectation is that in terms of customers or individuals enrolled in the scheme, eventually that will reach about 60 million. We will, however, have to hold records in the scheme on people who have left the scheme.

Q313 Bob Spink: How many points of access to the scheme will here be?
Ms Courtney: I would like to clarify that we are not talking about access to the system. I think that word is often used and misconstrued. We are talking about designing a system here which allows people to present identity information and have it confirmed.

Q314 Bob Spink: We are finishing very shortly and we only have 30 minutes. Could you just address the question specifically and, if you need to add to it, perhaps you could write to us.
Ms Courtney: I cannot give you a number or the volume of verification transactions that we would expect to see on the system.

Q315 Bob Spink: At every airport and port of entry in the country, at police stations and at social benefit offices and so on, how many points will there be in the country in the whole system?
Ms Courtney: We do have assumptions around this. It would be better if I offered to write to the committee.

Q316 Bob Spink: Can you just give us a rule of thumb now?
Ms Courtney: I will not be able to do that.
Chairman: We are happy about your writing back to us on that.

Q317 Bob Spink: Clearly, you said that the success in matching was fairly high, in answer to Dr Turner. Could you also say for each of the systems—iris, fingerprint, face recognition—what "fairly high" actually means? Could you write back to us on that, too?
Ms Courtney: Yes, certainly.

Q318 Bob Spink: Things are changing. I have learnt something this morning. It is now not a fused biometric system; it is a pick any one from three system. Do you think that if that is the case, if it is just pick one from three and try to match it, this will limit the ID card system's ability to deal with immigration, crime, terrorism and ID fraud?
Dr Bloomfield: I would go back to the conclusions of the 2003 NPL feasibility study, which recommended that, in order to differentiate between all the individuals in a population of 50 million, enrolling four fingerprints would be sufficient or enrolling both irises would be sufficient. The conclusions of that report were that you could use either four fingerprints or two irises in order to discriminate amongst individuals in a 50 million population. I think the answer to your question would be no, that how we choose to combine these biometrics would be sufficient to identify individuals from the population.

Q319 Bob Spink: In answering my colleague who asked for the limitations, you did not say what the limitation on iris recognition would be, for instance for women who were in menstruation where the rejection rate increases very dramatically, as I am sure you are understand, or on fingerprint recognition for people who are over 60, or bank clerks or teachers where fingerprints fail, as we saw with our Chairman who got two out of three failures since he was a teacher on a straight one-to-one fingerprint recognition in America a couple of weeks ago. Perhaps you will write to us about that as well. The whole policy of ID cards is predicated on an assumption that the technologies will work eventually: is that true?
Ms Courtney: The decision on the policy on ID cards was taken by the Government on the basis of quite a lot of analysis and the technology was only one aspect of that. Certainly the advice that we have received all along has been that the technology will be fit for the purpose to support the business objectives.

Q320 Bob Spink: So there is an assumption that the policymakers are taking that the technology will work? That is an assumption?
Ms Courtney: It is an assumption based on expert advice that was gathered at the time.

Q321 Bob Spink: Why have you not trialled the technology to find out whether it will work?
Ms Courtney: We have been trialling the technology.

Q322 Bob Spink: The 2005 trial was not a technology trial. There has been no large-scale trial on any scale at all that is comparable to what we are going to do of the biometrics. In fact, we do not even know what biometrics we are going to be used yet.
Ms Courtney: Trialling the system that suppliers will be proposing during the procurement phase of the scheme will take place during the procurement phase of the scheme. We cannot trial a system that we do not have yet, if you see what I mean. We have lots of experience from other operational systems: IDENT 1, NAFIS, other systems at the Home Office that operate on a very large scale quite successfully.

Q323 Bob Spink: When will you be trialling, how will you be trialling, and what is your budget for trialling?
Ms Courtney: I have to say that all of that is actually subject to us receiving the Royal Assent on the legislation.

Q324 Bob Spink: Let us then make an even bigger assumption than you are making on the technology. Let us assume that you will get, with the majority that the Labour Government has currently, Royal Assent. What is your budget for trialling?

Ms Courtney: We have not published our budget for trialling. It is part of the cost of the scheme. We will be putting information about the plans for trialling into the public domain once we are able to begin the procurement process, which we cannot begin prior to Royal Assent.

Q325 Bob Spink: Do Ministers know the cost of trialling? Have you given those costings to Ministers?
Ms Courtney: Ministers are aware of all of the costs of the scheme, yes. The costs of trialling are included in our business case.

Q326 Bob Spink: The scheme will be off and running by 2009. We are now in 2006, so we are looking at a couple of years. When will the trials start?
Ms Courtney: We have said all along that at a suitable time after Royal Assent we will begin procurement of this main technical component of the scheme, the National Identity Register and the biometric subsystems that support it. We have made the assumption that the process of procurement, including the trials, will take somewhere between 15 and 18 months in order to make sure that we are giving sufficient time to operate those trials as part of that procurement process.

Q327 Bob Spink: As a serious group of professionals you cannot sit here and look this Committee in the eye and tell us that you have not even started the trialing of the technology yet and yet the system will be up and running in two and a bit years' time. Surely you are not telling us that.
Ms Courtney: I was not saying that. I was saying that the procurement process, which included running trials of the specific solutions that the bidders would be proposing, we are expecting to run for somewhere between 15 and 18 months and it cannot begin until after we have had Royal Assent on the Bill and also passed gateway reviews and a number of internal health checks.

Q328 Bob Spink: Given all of these caveats, the massive IT infrastructure project and the need to trial the technology and the lack of technology and confidence in that at the moment, can you say what level of confidence you put in us having a system up and running and being used in two and a half years' time?
Ms Courtney: We have always said that the ready-for-service date for this system would be dependent on the solution that the industry proposes to us during the procurement process. I have a very high level of confidence that we will come to an agreement around the specification for that system with suppliers. The commercial terms there give us a high level of confidence it will be delivered when we have agreed they will deliver it. We have always said that we are working from planning assumptions until we are in that detailed dialogue with the industry.

Q329 Chairman: Would you agree that it is highly unusual to begin a procurement process before you have done the trials, yes or no? Can you think of any other major government project where you would begin the procurement process before you had done the trials?
Ms Courtney: I think it is quite important to point out—

Q330 Chairman: Yes or no?
Ms Courtney: I think it is not that unusual.

Q331 Chairman: That is normal government practice. What worries me here is that you are going to be entirely in the hands of the private sector in terms of this technology. You said in your evidence to us that it was not necessary to embark on publicly funded science related to biometrics and Tony Mansfield wrote in March that all systems need improvement. We have got a Home Office Biometrics Centre of Expertise who commission no research in this place, it is left entirely to the market. Is that acceptable?
Ms Courtney: I would not say that we have not commissioned research. We have commissioned research. We have a piece of research that the Home Office is funding right now into fingerprint biometric performance. I think what is important to say is that what we will be trialling during the procurement is the specific technical solution that the bidders are proposing for this procurement. What has been trialled before and what we have experienced from other operational parts of the Home Office is how other biometric systems operate, and they operate quite successfully. So it is not that the technology has not been trialled, but the specific solution for this cannot be trialled until the bidders are given an opportunity to propose it to us.

Q332 Margaret Moran: Given the very high number of high profile and large IT project failures there are out there, as we know from our own Audit Office reports, what scientific advice have you received on the lessons to be learnt from those failures? There are some large-scale IT projects which have succeeded. What research have you commissioned on those?
Ms Courtney: I hesitate to use the word research because what we have done is we have actually gone out and reviewed programmes, both programmes that have succeeded and programmes that have experienced difficulties. The National Audit Office has also published reports into this, the Office of Government Commerce has as well and the CIO Council under the Chief Information Officer for the Government at the Cabinet Office has also done quite a lot of work in this area. With most IT projects that may have experienced difficulty in the past we find it is not really the technology that is the problem, it is the other issues around organisational change, business process design, training, development and preparing both the users of the system and the operators of the system for implementation. We have certainly learned all of those lessons from looking at previous experience. The Home Office has had some very big successes in recent years. The Passport Service runs a complex system that successfully manages some 6 million applications for passports every year. IDENT1

under the Police Information Technology Organisation has been lauded as one of the best practice procurements for a major IT system that the Government has ever seen. I think it is quite important to point out that we are learning lessons all the time.

Q333 Margaret Moran: None of that is scientific advice. We have had evidence from the UK Computing Research Committee to say that the Government has made no real attempt to base computing policy on scientific evidence. You have listed the lessons from those IT projects but none of that is based on any scientific basis. With all due respect, the Audit Commission work is not an analytical research piece of work in the sense that you could learn lessons and apply them thereafter.
Mr Seed: You mentioned the Computer Society. The British Computer Society put out quite a comprehensive report on the complexity of IT projects and I was reading it last night while I was swotting for this! They listed the 10 most common causes of failure and me being the new boy in the project, I went through this and we have ticked the box and we have learnt from the Computer Society who are the experts in the field.

Q334 Margaret Moran: One of the things that they will have pointed out is the issue of scaleability. Given that this is the largest IT project of its kind, what research has been done on the scaleability of a project like this?
Mr Seed: We are doing that in a number of ways. We are doing it by comparison with similar systems. The FBI fingerprint database has something like 45 million records, so the numbers you can process are up there. The UAE has got in excess of a million records on iris. We know these large projects can work. We are in the process of commissioning a study from QinetiQ on data modelling to see just what the problems are with handling the volumes of data and moving it about and processing it.

Q335 Margaret Moran: What is the balance as between in-house scientific advice and industry advice?
Ms Courtney: We have our own internal advisers both from some of the more technical, deep science areas like biometric algorithms and also simply on technical operations, ie how you design a big system.

Q336 Margaret Moran: Could we have something in writing which lists who you seek the advice from and what the balance is as between internal and external industry advice?
Ms Courtney: We would be happy to write.

Q337 Margaret Moran: I understand two gateway reviews have been done so far. There have been complaints over the fact that commercial confidentiality has been used as a reason to prevent the learning from those gateway reviews becoming more public. We understand the issues around commercial confidentiality. Surely more information from gateway reviews, both past and into the future, could be put into the public domain so as to enable us all to have confidence or otherwise.
Ms Courtney: We have actually conducted more than two gateway reviews on this programme. We have conducted a number of gate zero reviews on the programme itself and also a gate one review on the business justification and we are now preparing for a gate two review on the readiness for procurement for the particular project around the technical systems. As you will know, the reports from gateway reviews are reports to the SRO of the programme, they are not intended to be put in the public domain. OGC is the channel through which lessons learned from other gateway reviews are fed into the other programmes that are going on around government. I do not think there is any risk of the lessons learned from reviews of our programmes being lost, but it is not through the process of placing gateway review reports into the public domain that that happens.

Q338 Margaret Moran: There have been arguments that you are not sharing sufficient information to enable industry or others to make this project work. Is the level of information that is being provided the norm in projects of this sort?
Ms Courtney: From the beginning of the consultation we have been consulting with industry about our plans. We have just concluded an in-depth market sounding exercise where we ran concept viability workshops sponsored by Intellect. We also had in-depth meetings with 60 or 70 individual suppliers. We have had in-depth meetings before that with specific suppliers in the smartcard biometric space in order to sit down with them and discuss our plans in some detail and seek their views on the feasibility, the practicalities and how best to go about engaging with the industry and procuring innovative solutions. I do not think that we have in any way run the risk of not being open enough with industry. I think we have applied best practice in this area.

Q339 Margaret Moran: We have been told it is often very unclear as to how that feedback makes its way into the specification, for example. Will you be making that transparent when you are publishing the strategy?
Ms Courtney: We will, yes. We have told the industry that we will be publishing our changed thinking as a result of the dialogue we have been having with them and making that publicly available to the industry and we will be doing that.
Chairman: From the Committee's point of view, we are wanting to see that there is an audit trail between the gathering of evidence—and that is why feasibility studies are important—and then, of course, a procurement process.

Q340 Mr Devine: I want to talk a bit about security and timescales and such like. In February this year a Dutch company claimed to have skimmed information off ID cards. I do not know if you are aware of that. Are reliability and security your highest priorities regarding the National Identity

Register? What other factors are influencing your decisions about the Register? Is there any scenario in which security levels would be sacrificed either for political reasons or for timescale reasons?
Ms Courtney: I believe that the Dutch company, as reported in the media, was talking about an early prototype passport that had been used and not an ID card.

Q341 Mr Devine: It still got access.
Dr Bloomfield: The people who claim to have cracked this prototype Dutch passport did it under laboratory conditions. You need to sit next to a passport with a reader for some considerable time to read it and get into it, which may not happen in ordinary conditions. The other point is that they had already quite a lot of information about the data on the passport which allowed them a foothold to get in through the cryptography and they were also provided with a number of consecutively numbered passports, which further weakens the cryptography. There is a fairly odd set of circumstances that they had in their favour in order to get through this cryptography. Having said that, being able to attack a card or a passport will get you, in the case of our identity card proposals, access to data which is not at all valuable. All the data, apart from the encoded biometrics, would also be printed on the face of the card and you would not actually get very much out of it. Attacking the database is a very, very different challenge.
Ms Courtney: It is important to point out that the accreditation process focuses on the security and integrity and also on the availability of the system. We need to make sure that all of our plans are accreditable not just against hacking and other security risks but that what we are designing here is a system that does not fall over, that does not have a single point of failure and it does not have a single point of decision-making and that there are clear audit logs of how the system is being used so that we can apply appropriate safeguards and supervision.

Q342 Mr Devine: And all this can be done security wise within a timescale of two and a half years, can it?
Ms Courtney: I am confused about the timescale of two and a half years—
Mr Devine: We are looking at 2009.

Q343 Bob Spink: That is the date of implementation.
Ms Courtney: I believe we have said that our timetable is indicative and that on current plans we are looking at 2008–09, but I have also mentioned that we are implementing a number of intermediate things that are happening this year, next year, in 2008, et cetera.

Q344 Mr Devine: You can write to us about that.
Ms Courtney: The actual date for "turning on" the National Identity Register is very dependent on the suppliers' proposals as they come back to us through the procurement process. If you would like me to say something more about the security approach, perhaps I can ask Nigel to expand on the security requirements.
Mr Seed: 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 team is embedded within my procurement team; they are fully engaged. They are on my back all the time, as they should be. The people who are going to do the accreditation are having meetings with our people all the times, looking at our requirements as they develop and then inputting to those requirements. 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 the way from very basic level access and flooding and losing it that way right the way through to hacking.
Ms Courtney: It is the security around the people, the processes and the systems, not just the technology.

Q345 Mr Devine: There is a claim that basically if you have one database you are creating a "honeypot" for criminals to hack into. How would you respond to that suggestion?
Ms Courtney: First of all, I think that is an assumption that there is one database. We have not predetermined the architecture of this system. Our security requirements include issues around making it difficult for people to hack in and access the system. We will have security accreditors throughout the lifetime of this scheme, not just in our planning phase. I think we are doing everything we can to ensure that the security considerations are taken very seriously indeed.

Q346 Mr Devine: You are not going to have one database, is that what you are saying?
Ms Courtney: People like to talk about the National Identity Register as a database. The National Identity Register will be a technical system that may involve a series of data storage solutions. I think it is important that people do not prejudge how the architecture of the system will be designed.

Q347 Chairman: I am now very confused as to what you are saying here. You will have a series of databases. Where is the evidence coming from as to whether you are going for one single database or a series of databases?
Ms Courtney: You are going to ask me questions about the technical design and I am not a technologist.

Q348 Chairman: Can any of your colleagues answer?
Ms Courtney: Our reference solution assumes one thing and then we are working with the market on options—

Q349 Chairman: In terms of phase one procurement, will the market also decide how many databases you have?

Mr Seed: To an extent, yes. We are doing an output-based requirement, so we are saying this is what the system must do. How they do it is not defined. If industry comes back and says one single monolithic database is the best way and it meets all the requirements then there may be one database. Equally, they could come back and say the security is increased by having partial data here and partial data elsewhere. We have not defined it.

Q350 Chairman: Will industry not come back with a solution that is best for them?
Mr Seed: Possibly.

Q351 Chairman: I would if I was a commercial company.
Mr Seed: Of course you would. You have got to remember that this is an open competition. If somebody comes through with a cheaper solution, that is not necessarily what we are going to select. We are going to look for the best technical solution and the best value for money.
Dr Bloomfield: It is worth adding that it will also have to be a solution which meets the requirements of our security accreditors.

Q352 Mr Devine: Let us say Jim Devine's computer company gets the contract. I can set up a company in Scotland and send information to Scotland, Wales and London. I could outsource this contract to 100 different companies. Is that right?
Ms Courtney: We will obviously have a due diligence process—

Q353 Mr Devine: Is that right?
Ms Courtney: Not necessarily. We will have a say in this procurement process, as any government client does, about how the consortium is formed and who is providing the solutions. While we do not have an intention to dictate how the market responds to the requirements, we have made it clear that we have to take a decision based on the proposals they put to us. If they propose a solution that includes using companies in a subcontractor relationship such as you describe that we cannot have confidence in, we will not be signing a contract with them.
Bob Spink: Could I ask you to confirm again, please, because I am incredulous about this, that all of this will be up and running in two and a half years? Can you confirm that none of this will be outsourced offshore UK?

Q354 Chairman: Can you answer the second part because I think you have answered the first part to be fair?
Ms Courtney: We have offered to write back with the procurement principles that apply to that.

Q355 Margaret Moran: Is it not inevitable that the market solution will be a single database simply because of the complexity of joining up a myriad of departmental databases which do not match? How are you going to be able to evaluate what comes forward to you in that respect as against the option of multiple databases which may not come forward at all from industry?
Ms Courtney: I do not believe there is a foregone conclusion about that. In our market soundings we have had suppliers who have been working for some time on their own reference solutions for this and they have a number of different approaches, all of which may be equally valid and which should be evaluated in the open competition.

Q356 Mr Devine: You mentioned earlier on that technology is changing. It has been suggested by colleagues in America that these cards are going to be out-of-date very quickly. I think KPMG's assertion is that the durability of the cards would be 10 years. Have you made any assessment of that?
Ms Courtney: We did do that because that is one of the assumptions driving some of the costs in our business case model. We went out and did a survey of card manufacturers to look specifically at card lifecycles and durability and based on the evidence that they gave back to us we are confident in the 10 year assumption.
Dr Bloomfield: And also from looking at other schemes. Hong Kong, for example, has a polycarbonate smartcard which is valid for 10 years.

Q357 Chairman: Nigel, if you have multi-databases as part of your phase one procurement, and that is an option which is open to the tenderers of the process, who controls the data? Would it be the companies who win the contract or does the Government retain control of that data?
Mr Seed: It is a bit of both. The company will be running the database per se, but the data itself will be monitored by civil servants sitting alongside the contractor. We are intending to have a partnership agreement. There is no intention to hand this contract over and then walk away and leave it with a commercial outfit. There will be full-time civil servants in the data centre monitoring the data and the usage of the data.

Q358 Chairman: But a private company will be able to have access to all that data if they win the contract, will they not?
Mr Seed: By definition, in order to maintain the database, yes, they would have to be able to see the data on it.

Q359 Dr Iddon: As you know, this is a very excitable political issue and all the Members around this table get lots of correspondence on it. Apart from the libertarian arguments which we engage with, the second argument is about the costs and that is where I want to go now. Obviously the London School of Economics is in opposition to the Government on costs and they have quoted figures of £10.6 billion to £19.2 billion, which are the 10 year costs and which include running costs. We can argue about those figures and they have been argued about and the Government has contradicted them. The hon Member for Leigh has quoted a figure of £584 million per year as the total cost but he will not

reveal the estimates within that particular figure. Obviously those figures are way apart, there is no similarity between them. I just want to examine that big difference. How can you be certain about the costs when you have not even set a detailed specification yet?
Ms Courtney: We have had to produce a reference solution for ourselves in order to evaluate what the likely costs would be. We have done that work based on the feasibility analysis that we have done. The figure of £584 million—

Q360 Chairman: That is not credible if you do not mind me saying so. I think I speak for all my colleagues when I say we find that the most incredible statement given the evidence you have given us today about the state of this project.
Ms Courtney: Our cost assumptions have been independently audited by KPMG and so we can have quite a high degree of confidence in them at this point in the development of the scheme. We have had Treasury scrutiny of our cost assumptions, we have had the Group Investment Board scrutinising our assumptions, and we have had the independent assurance panel who advise our programme board review all of our approach to this and the OGC has conducted a gateway one review of our business case, so we do have confidence in our cost modelling. The final costs of the detailed component of the scheme we cannot finalise. We will not know what they are until we have conducted, subject to parliamentary approval, an open procurement process, but we have been quite conservative in using all the Treasury Green Book guidance, using optimism and bias and building contingency assumptions in. We are quite confident in our cost estimates.

Q361 Dr Iddon: The £584 million figure is a hard figure.
Ms Courtney: Those would be the year-on-year running costs of the scheme and it includes the costs of running the Passport Service which are very well known because that is an existing operation. We are able to forecast the volumes of passports and the costs of issuing passports quite accurately. The National Audit Office has always given a clear green light to the Passport Service's accounts. The largest proportion of the £584 million is the costs that we feel quite confident we can project.

Q362 Dr Iddon: We accept that and hope sincerely that you are right with those costs. What is wrong with the LSE costs? Have you examined those in detail?
Ms Courtney: We have examined them in detail and we have published some information on our website which is a response to the assumptions that were made. The costs modeling behind the LSE made a number of fundamental assumptions which were very different to our own proposition. They made assumptions that ignored the Passport Service as an existing operation and they made assumptions that people would be required to go through, for instance, a full registration process if they were to report their ID card lost or stolen, that sort of thing. So there were a number of factors in their cost assumptions that drove their cost assumptions up which simply are not realistic in view of what we are actually proposing.

Q363 Dr Iddon: We have not had a break down of this £584 million figure. As I said, the Minister will not reveal the estimates within that figure. Are you able to supply the Committee with a full break down of that £584 million figure so that we can examine it?
Ms Courtney: We have stated that about 70% of that £584 million relates to the issuing of biometric passports and the rest is an incremental cost for issuing ID cards to a larger proportion of the population and includes the cost of producing the card itself. The vast majority of the costs are the process for registering an identity and issuing a passport.

Q364 Dr Iddon: When you eventually go to procurement are you expecting that figure to increase significantly?
Ms Courtney: As I said, we have built optimism bias and contingency into our own cost assumptions so we are not expecting it to increase.

Q365 Dr Iddon: That is a pretty hard figure you are telling the Committee. As MPs we have a degree of scepticism about government procurement projects for IT. We have seen costs escalating phenomenally in some cases when Government has procured the technology. You can understand why MPs and the general public out there are very sceptical and perhaps will be sceptical about what you are saying this morning, although we accept you are saying it with great sincerity. If the project gets out of hand for some reason that you have not even foreseen yet, has the Government set a ceiling above which it will not go to take ID cards out for public use?
Ms Courtney: I believe that ministers have stated several times that they will not be taking a scheme out to the public that was unaffordable or set a fee for the public that was unacceptable. There are many decision points between now and actually introducing the scheme. As I said, there will be many opportunities to review that our cost assumptions are correct. You will know that the current legislation before Parliament has included an amendment that will have us put a report before Parliament of our costs on a six monthly basis, so there will be plenty of opportunity to review.

Q366 Margaret Moran: Some of us accept that the LSE assessments are risible, but I fear we may be having the same perception right now. Have you included in the figure that has just been quoted the costs of dealing with the interoperability or the lack of interoperability of different databases, assuming that one of the options will not be a single database but many?
Ms Courtney: I did not mean to imply that a solution might involve stringing a number of legacy databases together. That has never been part of this

proposition. We have always said that our requirements are for a data repository that could be populated one record at a time.

Q367 Margaret Moran: So the costs include multiple databases.
Ms Courtney: The costs include a reference solution for checking people's identity information, which does include reviewing data sources from public and private sector sources. I think we have been quite clear about that. We have looked at the costs of being able to do that interface with other databases in that respect. The costs include processing application information, recording details, such as biometrics and personal identity information, name, address and the like, storing it securely and being able to verify that information back to an accredited user of the system. The costs include all of those inter-operability requirements.

Q368 Chairman: Katherine, you mentioned the KPMG report and I have it in front of me, which was produced on 7 November 2005, and it clearly states that the performance of the biometric matching drives a significant amount of cost and I think you would agree with that. It then goes on to say, "We recommend that the IDCP team should have further discussions with the USVISIT programme to gain detailed insight into the cost drivers for this area and the UAE to verify the cost and performance of the fingerprint and iris hardware matches respectively." They still had real questions about the cost assumption. Have you been to those places, both the UAE and the USVISIT, as KPMG recommended?
Ms Courtney: Since the KPMG report?

Q369 Chairman: Yes.
Ms Courtney: We have not been.
Mr Seed: I will be going on 9 April.

Q370 Adam Afriyie: There are huge risks. My background is in technology for 15 years. The Head of the e-Government Unit, the Information Commissioner, the industry and probably all of us here instinctively know there is a huge risk the technology will not work in the form in which it may want to be deployed in the next 18 months. Would you stake your mortgage on the fact that within 18 months of starting this scheme it will be up and running and it will work? As soon as you have got permission to do your technology roll-out, will it be fully up and ready for use within 18 months?
Ms Courtney: This is a long-term development scheme.

Q371 Adam Afriyie: I will take that as a no!
Ms Courtney: We have the biometric visas rolling out over the next year or two years, we have biometric residence permits rolling out and we have the biometric passports. We introduced the first electronic passport only this month, that was when the first one rolled off the production line. All of these things are testing the technologies that are the building blocks for this scheme. By the time we come to launch this scheme I am very confident that we will have sufficiently proved in an operational environment the components of the scheme.
Adam Afriyie: Within 18 months?
Chairman: May I thank Katherine, Nigel, Henry and Marek for what I think we would all agree has been a very interesting session this morning. We are genuinely interested in representing the House on this issue. Thank you for your contributions.

Wednesday 3 May 2006

Members present:

Mr Phil Willis, in the Chair

Adam Afriyie
Mr Jim Devine
Dr Brian Iddon
Margaret Moran
Dr Desmond Turner

Witnesses: **Mr Nick Kalisperas,** Director for Markets, Intellect, **Mr Jerry Fishenden,** National Technology Officer, Microsoft, **Mr Dave Birch,** Director, Consult Hyperion, and **Professor Martyn Thomas,** UK Computing Research Committee, gave evidence.

Q470 Chairman: Good morning, everyone. Good morning in particular to our first panel of expert witnesses: Nick Kalisperas, the Director for Markets, Intellect; Jerry Fishenden, the National Technology Officer for Microsoft; David Birch, Director from Consult Hyperion; and Professor Martyn Thomas from the UK Computing Research Committee. Welcome to you all and to our visitors and members of the press this morning. This is our second session on our identity and technology case study, which is part of our broader inquiry into looking at the way in which scientific advice helps government to set policy, to deal with the issues of risk, and the whole issue of evidence-based policy which is our major inquiry going on. Our purpose this morning is mainly to look at process. We are not in a position as a committee and nor have we set up this inquiry to make judgments about specific technologies or whether in fact the ID Cards Programme is right or wrong. That is an issue rightly for Government. Our issue is to say: Where is the evidence to say you will meet your stated objectives behind that? That is the purpose of this inquiry. I wonder if I could invite you, Nick, to chair your panel. In case there is a need to chair it if things get riotous, then we will call on you to get your colleagues into order. Perhaps I could start by saying that the Identity Cards Programme team said that they have "consulted widely with experts". Do you agree?
Mr Kalisperas: They have had some consultation with experts.

Q471 Chairman: That is different from "widely".
Mr Kalisperas: Yes, it is. Having read the submissions, there are clearly some groups which have not been consulted. I would say there is a difference between consulting widely and having regular consultation. I think, as we approach procurement, there should be more intensive consultation specifically with the industry, so that the industry has a full and clear picture from which they can decide whether to bid for this programme or not.

Q472 Chairman: That is a fairly critical start, if I read between the lines there.
Mr Kalisperas: We are looking at a programme which carries significant reputational risk for the IT industry. We have had an ongoing dialogue with the Home Office for at least three and a half years as the Bill was going through Parliament, particularly towards the third reading, where there were a number of votes that potentially could alter the structure of procurement, that there needed to be better interaction with the IT industry, not just potential prime contractors but also those further down the supply chain, in order for them to make clear assessment as to whether they believe this project was worth bidding for or not.

Q473 Chairman: Dave, would you agree with that? What is the position on consultation? Has there been sufficient? Has it been wide enough? And what more could the Government have done?
Mr Birch: I think I would raise the question of what the consultations were about. If you are consulting industry about whether the card should be red or green, that is very different from consulting industry about whether there should be a card. A lot of the consultations tend to be discussions about the structuring of procurement and how exactly the procurement would work, and not really the kind of consultation that you would expect at a more scientific level, consultation about how the scheme should work overall and what it should do. There have been some consultations. The major consultation that I attended with Intellect, frankly I thought was a little disappointing. Most of the presentations were just telling us that this is how it is going to be, followed by an injunction to get out and do something about there being too much sort of negative publicity—and I cannot remember the exact phrasing. I do not think it was really consultation in the sense that you are thinking consultation constitutes.

Q474 Chairman: This is a pretty big project.
Mr Birch: Yes, of course.

Q475 Chairman: Martyn?
Professor Thomas: From the point of view of the technology, I do not think there has really been any consultation with the academic community. The academic community is independent and therefore can bring something to a consultative process that industry really cannot because we can stand back as independent academics and look at the viability of something and look at best practice without having a vested interest of any sort. We are not trying to sell anything, other than to try to get people to use the best possible science. From my perspective, any

involvement, any consultation started in the wrong place. It is still, as far as I can see, unclear what the objectives of the overall programme are and how it is envisaged it will deliver the supposed benefits. The benefits are not quantified. They are drawn extraordinarily widely and yet are put in terms of help towards this and benefit for that. In most cases, it seems to me, there is no basis for arguing that the sort of programme that seems to be emerging will deliver those benefits, either in a significant way or that it will necessarily be the best way of delivering those benefits if you started with a completely blank sheet of paper. I feel that the consultation did not start at the right level, with stating what the really desired outcomes were at a system level, at an overall societal system level, and then trying to work through to what the right solution would be. It came in with a solution, and then started to pull in lots of benefits, it seems, almost to try to justify the solution that had been partly adopted.

Q476 Chairman: Jerry, do you feel the industry has been completely open with the Home Office regarding any possible problems with the scheme?
Mr Fishenden: We have certainly endeavoured to be, both at the Intellect meetings and through direct contacts with the Home Office. I would reinforce the point that the consultation became unduly focused, in my view, on procurement issues. I think the industry was looking for the opportunity to understand the types of scenario technology needs to support, and to debate fairly openly and with each other how the technology might actually deliver against those scenarios. Every time we came close to wanting to talk about the architecture, we were told that was not really up for discussion. That because there was an internal reference model that the Home Office team had developed themselves, that they did not feel they wanted to discuss their views of the architecture. I think the phrase they used was that they did not want to "stifle innovation" at the time they got to bid phase.

Q477 Adam Afriyie: To be absolutely clear, you are saying that they refused to show you their architectural framework document for delivering this project.
Mr Fishenden: In terms of technical architecture, yes. There were some requests from the industry to have sight of the reference model, because it is sort of implicit in a lot of what they have been talking about.

Q478 Chairman: Was industry involved with developing that reference model?
Mr Fishenden: As far as I know, not—because it was not discussed at any of the industry consultation groups that I went to.

Q479 Chairman: Where do you think the Government got its advice from?
Mr Fishenden: I presume from its own internal and external consultants that it recruited to the programme.

Q480 Chairman: I thought you were consultants.
Mr Birch: No.
Mr Fishenden: No, we are not consultants.

Q481 Chairman: Are you not able to give them that consultancy advice on the basis of industry or academia?
Mr Birch: We are ready and willing to do so.

Q482 Chairman: You are capable of doing it but you were not asked.
Mr Birch: Yes.

Q483 Chairman: One of the criticisms that could be levelled—and I am doing this innocently, as you realise—is that industry has such a vested interest in what is going to be one of the most significant commercial projects, that it does not criticise strongly enough.
Mr Fishenden: There is the reputational point to which Nick alluded earlier. I do not think anyone in industry would like to be here in two, three, or five years time, whatever the time scale might be, explaining why yet another major public sector IT project has gone off the rails if that were to happen. I do think there has been a consistent willingness on the part of industry to engage in open dialogue with the Home Office. But as we have been saying, I think the focus seems to be very much on the consultations around procurement related processes and structures and not to do with a wide, industry consultation on the technology and the type of scenarios that the technology will need to support.

Q484 Adam Afriyie: Are you aware of ways in which your advice or industry advice has been incorporated into the project?
Mr Kalisperas: Not at the moment. Not until we see the OJE notice and statement of the requirements will we have an accurate position of how our advice has been incorporated into the procurement.

Q485 Adam Afriyie: Does anybody else have any observations? So there is no visibility yet as to whether any advice has been taken or input received. Martyn Thomas, the UKCRC have said in written evidence that "Government has made no real attempt to base computing policy on scientific evidence" and you have echoed that again this morning. What led you to that conclusion?
Professor Thomas: The way in which government procurement is carried out—indeed, the way in which most IT procurement is carried out—is essentially based on technology that is 30 years old, which in an industry that is only 60 years old is pretty shocking. The extent to which requirements are drawn out and written down in a way that you can reason about, analyse for real weaknesses, and the extent to which really sound computer science is brought into the technology, so that, for example, you are not building computing systems using technology that has known security vulnerabilities which are completely avoidable but which are just commonplace and regularly incorporated in new systems, all these things are indications of a woeful

lack of proper scientific foundation for the procurement and indeed implementation of IT at the moment.

Adam Afriyie: Do the rest of you agree with that?

Q486 Chairman: That is a fairly damning comment.

Mr Birch: I think it is fair to say that for large projects like this it does sometimes look as if the fundamentals of it are a little backward looking. The imagination comes from a rather 1960s world of just the giant mainframes and terminals connected to them and so on. I think that is valid. I think the origin of it is a little harder to pin down. You are taking this evidence and it must be transparently obvious to you that there is a systemic issue on large procurements like this, whereby—and I am not picking on anybody—if you are a large supplier and you make widgets and the Home Office say, "We are thinking about implementing a gigantic system of widgets" then of course you say it is a great idea, and then the discussions very quickly move into the intricacies of the procurement: "How exactly are you going to procure the widgets? What is the time scale" and so on. And the kind of scientific evidence about whether you need widgets in the first place is complicated. It is necessarily quite difficult. You have people who are, frankly, scientists giving evidence to people who are, frankly, not, and so if you have a discussion about—I do not know—what the lifetime of the next 509 certificate should be, it is just gibberish to most of the people in the room. There is a systemic problem that needs to be addressed there which is not just about the ID cards programme, although obviously that does highlight a lot of the issues.

Q487 Dr Turner: What you are saying rather chimes with what this Committee has raised at other inquiries with other government departments, the concern being that the department concerned does not have sufficient scientific expertise located within the department to act as an intelligent client to procure highly complex systems or new science or technology. It rather sounds from the tenor of your evidence that this is a criticism which may currently be valid for the Home Office. Do you have a view on that, Professor?

Professor Thomas: I believe that is generally true and specifically true for this programme. It is quite difficult for a major department to have the right level of skills for all the procurements. One of the ways that has been suggested to break through this problem, recommended by the Royal Academy of Engineering, is the introduction of what they call "system architects"; the idea being that, in the same way as an architect sits between the client who wants a new major building and the builders, the construction people, the engineers who will develop that building, and works out with the client what the requirements will be, how the business will be affected by the new system that is being procured, in exactly the same way, you could have a system architect come in for major IT systems, to work in a very technical way with the potential suppliers but in a very business-oriented way with the client and do the translation, so that the architect would capture the business requirements and turn them into a very rigorous specification before they would be put out for competitive procurement. The benefit of that would be doubled, because, firstly, you would take quite a lot of risk out of the procurement process, and also you would be able to introduce smaller companies into these major procurements. The system architects would typically come from the innovative smaller companies that are using the more advanced technology for doing things like requirements' analysis. At the moment, the major procurement structure stifles innovation because it is very hard for the innovative, new, smaller companies to get into the market. As the public sector is more than half the market for IT services in the country, that is a major impact on the structure of the industry.

Q488 Adam Afriyie: I have a slightly acerbic question. To what extent do the complaints from the industry, from Intellect and others, including yourself, stem from the fact that you have been ignored during this particular ID card project?

Mr Kalisperas: Personally, I do not think that is the case. Our responsibility is that we are not-for-profit and we are a technology-neutral trade association, so the only thing we are interested in is getting procurements right and learning lessons. If we did not think a procurement was being undertaken in the right manner, I feel, having spoken to our members, that it would be a dereliction of our duty, our responsibility then, given that we are also safeguarding their reputations as well, if we did not speak out.

Professor Thomas: UKCRC is increasingly frustrated by the fact that major IT procurements go wrong for entirely avoidable reasons. The UK is world class in computing science. We could be in the forefront of the world in developing, building, procuring new systems, if only we were prepared to base those activities on our world class position in computing science. For a variety of reasons, nobody seems to want even to engage in conversation with the academic community about a programme of work that could bring about that transformation. We are not selling silver bullets; we are suggesting that the systemic problem to which Dave Birch referred could be cured over a period of years, and the result would be that it would save the public sector billions of pounds a year. For some reason, nobody wants to engage with that agenda.

Mr Birch: Could I answer Adam's question, because I think it is an incitable question, because it is a genuine human emotion to think that you have a better idea for how to build the system—which actually I do, but that is not the point! Martyn's point about the architect, I would prefer to be seen as defending the industry. We get a lot of criticism about all of these projects continuously going wrong: nothing ever works properly; it is all a total waste of money—whether it is child benefit or things for farmers or whatever. I just want to make the point that it is not our fault, because when the government procures buildings with architects—the

Scottish Parliament, for example—they are late and cost too much. It is not just because we are IT people; it is because of the way these things are approached. It is a more genuine systemic problem.

Q489 Margaret Moran: You have talked about a lack of consultation around specifying the technologies, when we have heard evidence from the Home Office that they do not want to curtail industry, they do not want to define the technology itself. Is it not contradictory that you are complaining that the Home Office are not sufficiently specifying the technology, when they are leaving that to you? Should it be business that specifies the technology?

Mr Kalisperas: I think there is a balance that needs to be struck between leaving a certain amount of innovation open to the market but being able to provide the very basis of a framework through which industry can work. We have seen from recent government procurements that have been cancelled at very short notice, having taken 15 to 18 months, that a procurement process can cost a company upwards of one million pounds in just procurement costs. Those are costs that are not going to be recovered. The one thing that we want to make sure of is that there is sufficient framework there for companies such as Jerry's or Dave's to make accurate decisions on how they want to respond to a particular procurement, what sort of technologies they want to put forward. If you just say, "We are going to leave it to the market" that is just too broad. There has to be the outlines of a specification there.

Mr Birch: Could I argue with you about the question? It is not being left up to the market; it is in fact very prescriptive. It is already decided that there will be a smart card. It is already decided that there will be a register that is going to store your address and all sorts of other things. All this stuff has already been decided. Just to picture it at a slightly higher level, if you said, "We, as the Home Office, feel that some form of national identity management system would be appropriate in a modern economy"—which I have to agree with—"Let's have a consultation about what it should do and so on" that is not the same as saying, "We are going to have a gigantic registry somewhere and we are going to have all these smart cards. Can you consult with us about what colour they should be" or something. It is a mismatch of levels there.

Mr Fishenden: I would like to add that there is something contradictory happening here. I take Nick's point that the proof will be when the procurement documents come out and we can see how outcome-based it is and how prescriptive or not the actual procurement intends to be. But I think an opportunity has been missed to evaluate alternative options for delivering those outcomes. Although I noticed that when you took evidence a few weeks ago from Katherine Courtney and her team they said it will be outcome based, in a lot of their other answers they were saying, "This is the way the card will work . . . It will have this on it, it will have that on it. It will work this way, it will not store this," and you think: "Is it prescriptive or not?" I have to say that the jury is probably out until we see the formal procurement documents as to whether it is entirely outcome or scenario based around the types of behaviour, if you like, that you want to see from an ID card system. I was looking yesterday on the website. The few scenarios they do have mapped out at the moment I think still exhibit an interesting level of understanding. There is one talking about somebody who is 18 going into an off-licence and being able to assert proof of their age, and a 70 year-old looking for a 65 year-old discount. It then goes on to describe how the ID card will be used to reveal their date of birth in order to prove their age. To me that just highlights the type of issue we have been trying to flag up for the Home Office: Why would you want to reveal somebody's date of birth in that scenario? You would want to reveal their age; their entitlement that is, that they are over 65. You do not even have to reveal their age, but that they are over 65. If you start revealing things like their date of birth, then I think the banks and everyone else are going to have a huge headache. Because, what do they ask you when you phone up to access your online account? It is personal information like date of birth, but that scenario has just said that you are going to start handing that type of information out every time you use the ID card. It is that type of debate which I think concerns the industry, that after all these consultations we still do not seem to have had an impact on the level of understanding about what makes for good identity systems to practise.

Professor Thomas: There is a distinction that ought to be kept quite clear between identity (in other words: Who are you?) and authentication (What are you entitled to do?). When what you are asking for is authentication (Are you allowed into the country? Are you entitled to benefits? Are you of an age to buy alcohol?) you do not need to know who the person is. If you go that extra step to ask for identity information when what you actually want is authentication of a right to do something, then, firstly, you are violating privacy issues, but also you are revealing information which makes things like identity fraud much more likely to occur. If you start then tying authentication into biometrics which cannot be changed if they are compromised, then if you start getting those stolen electronically and using them for remote authentication, customer-not-present type authentication, you will create a security nightmare where somebody's biometrics are no longer available to them to authenticate themselves for the rest of their lives.

Q490 Margaret Moran: In summary, you are saying that lack of consultation could open up the system to greater vulnerability.

Professor Thomas: Exactly so.

Mr Birch: To reinforce Martyn's point about the distinction between scientific evidence and what the general public thinks about it, if you see what I mean, that is a very good example, the ability to reveal credentials of an individual while simultaneously hiding their identity. To understand how that works, you have to understand a certain

amount about cryptography and digital signatures and blinding and so on and so forth, so there is a distinction between what the scientific evidence will be saying in that case and what in general opinion—which in some cases can be very paradoxical—can be achieved with the technology now. One of the reasons why I am rather in favour of an ID card is because it is a way of creating privacy where none existed before, but, in order to understand how that all comes together, Martyn is right, you have to layer these things. A consultation which says, just to take a simple example: Should your name be on your ID card or not?—a very simple and very fundamental question—what consultations have there been about that? Personally, I would say none, but I stand to be corrected. Basic fundamental things like that are what should be part of that consultation process. There is scientific evidence, I am sure, from other countries to say why it might or might not be a good idea to have the name on the card, but that is not the kind of consultation that has been going on. The consultation that has been going on is: We are going to have a card, we are going to have a name on the front, what is the best way to procure it?

Q491 Margaret Moran: You are illustrating the point you made before about your concern about lack of Home Office expertise, but, given that we have been told by the Home Office that the decision around technology innovation will be industry, do you think the Home Office has sufficient expertise to be able to evaluate what comes back from that process?
Professor Thomas: It seems unlikely.

Q492 Margaret Moran: Shall we take that as a general no. That seems blunt and to the point. Shall we go back to the technological architecture? We have been told in our evidence that is interdependent with the business case. Do you think that is the case? Do you all agree that there is clarity about the aims and uses of the project that we are talking about?
Professor Thomas: It is clear that the technology is interdependent with the business case because the business case is founded on the requirements and the technology should be there to support the requirements. The requirements are woefully unclear, in my opinion. Everything that I have managed to find on the web or in other documents that I have seen about the programme, lays down a set of aspirations for the ways in which the identity scheme might contribute to reducing fraud under some circumstances, but there is no quantification, there is no analysis of how the proposed scheme is going to make that kind of contribution, and you would need to get into some detail, about how it would be envisaged that the system would be used, before you could do any real analysis of whether that is the right solution to solving the problem that has been laid out.

Q493 Chairman: Jerry, do you agree?
Mr Fishenden: I think there were only three scenarios on the website yesterday as to how this card might be used. I have mentioned one of them already. I am concerned about aspects of even that scenario and the fact that it could lead to greater ID fraud risk. I would have expected at this stage to see a fairly rich set of very precise scenarios about exactly where and how the ID card would be used and to address many of the issues we are talking about here as to what gets released in those types of scenario. That is still not prescriptive on the industry in terms of specifying the particular technology or how we do it but it does set some policy requirements about making it desirable not to unnecessarily reveal identity information when that is not necessary for that particular scenario.

Q494 Dr Turner: Can you gentlemen, with your breadth of experience of large scale ICT projects, remember any other comparable case where a project has been discussed at public and political level for so long and in such detail in Parliament, yet is surrounded by such lack of decision as you have pointed out, Jerry, in the kind of scenarios that will be associated with its use, least of all any ideas of technical specification? I cannot remember anything comparable. Can you? If so, can you draw any conclusions?
Mr Kalisperas: This goes to the heart of government procuring and how government behaves as a customer. Dave has talked about a national identity management scheme. This is not it, for the simple reason that what we have here is a reflection of the silo mentality that exists with the public sector. What we have here is the Home Office procuring a national identity card scheme but only within the boundaries that the Home Office can do. When we first engaged with the Home Office three and a half years ago, it was called an entitlement card, and we wrote a paper which currently exists on our website which said that we saw an entitlement card as the natural evolution in the modernising government agenda but that for that to happen it required joined-up government, it required departmental cooperation, and it required a central owner to drive it forward. We do not have that now. We have a card that is very much reflective of the Home Office's own objectives and aims. What concerns us is not the fact that there is a lack of clarity but what is the future planning for this card. Once it is rolled out, whenever it is, 2009–10, how else will the card be used and what level of interoperability will be built into that card? What are the specifications in terms of standards? How else does the Home Office see this card evolving? Hopefully, by then, there should be a level of departmental cooperation which should—touch wood—mean that the card would be used for more than just identity but would also enable people to access public services. That is not here. We regard that as a missed opportunity. We said it three and a half years ago and we are saying it now.

Q495 Dr Turner: You are saying that, if the Home Office were to be acting as, shall we say, the lead department for a group of departments procuring this for the wider application of the group, we might be looking at something different.

Mr Kalisperas: I think we would be. Also, I think in that regard, in terms of building public trust and confidence in the scheme itself, you would probably get a slightly more favourable response. At its basis, I think we have a lot to learn in this regard from the financial services community about how they moved from signature on credit cards to chip and pin.

Q496 Dr Turner: Can you give us some of your views about the best way to organise the database. What is the best option for the database? Is it one big, massive mainframe somewhere in Birmingham or should it be a network of loci? Has the Home Office consulted you on the architecture of the database?
Mr Birch: No, to answer the second question first. We are going to start sounding like broken records here, but you cannot answer the question about how should we organise it until you know what the requirements are. To reinforce Martyn's point, there is a scientific distinction between the kind of stuff that you have written down here and a requirement. If you say that the database should be secure, for example, that is not a requirement, that is a goal. It is aspirational. If you say the database must weight five kilograms, that is a requirement. Something that can be tested and measured and assessed, that is a requirement. We do not really have any requirements, we have goals. I agree that some of them are quite aspirational. "Let's just take that as read" is the introductory answer to every question. Until you know the requirements, it is very hard to say. I would say that if you want to minimise risk around the database—which I think is what is behind the question, if I have understood the briefings properly—I cannot see how that can be done inside the current structure, because there are no obvious reasons why you want to store any of that data at all, frankly, as far as I can see. The purpose of the register is to ensure the uniqueness of the identities. That is its logical purpose, which is really to do with storing biometrics. I can understand the reason why you want a database that stores the fingerprint and irises, because you need to ensure the uniqueness of the entries. I do not really understand why you would want to store names and addresses or previous occupation. I do not get it. That was just made up in the Bill—if you know what I mean. That was just said in the original Bill, that it has to store your inside leg measurement or whatever. That is not the outcome of scientific process.

Q497 Dr Turner: Does that aspect increase the risk of skilful abusers of the database?
Mr Birch: I think the risk was already 100%, so, when you say "increase the risk" I am not sure it makes any difference. The risk to those kind of databases, which is transparently obvious in the case of things like the DVLA and the Criminal Records Agency, is not that some Russian Mafia mathematical genius is going to find some new prime number and—

Q498 Chairman: We are coming back to the issue of risk.

Mr Birch: The risk rests with the fact that it will be your own staff.

Q499 Margaret Moran: I am assuming that we are all agreeing that we are in the pre-procurement stage. What opportunities are there for the issues that you are raising now to be factored into the discussions? Is it all too late to have the kind of scientific advice to which you are referring introduced into the process?
Professor Thomas: It will be necessary to have a detailed specification and to have it reviewed if this is going to be a successful project. It is never too late to do that. If we carry on down the path that we seem to be going down, it may be that this system will fail completely and it will have to be re-introduced in 10 years time and then that process will be gone through. But until it has been gone through the programme will not succeed.

Q500 Margaret Moran: Is that the consensus?
Mr Birch: Because none of us has seen a requirement specification, it is kind of hard to answer that question. My suspicion is that, as currently constructed, it probably is a little late. But, then again, you MPs might all vote not to have one tomorrow and then we can start again and have a better crack at it.
Mr Kalisperas: I think I would agree with Martyn that there is enough time, but you would have to take the politics out of it, the sort of politically driven deadlines that say a card needs to be introduced by 2009, that procurement needs to be done by then. I think you have to take that out. Civil servants and the industry need to be listened to, if, in the views of those individuals, it is not feasible in that time to allow enough time for consideration of the specifications and also enough time for testing, analysis and whatever. All of that needs to take place and if 2009 is not achievable then ministers need to listen to that and need to cast aside their own reputation in the short-term and look at the longer term benefits for the project.

Q501 Dr Iddon: The Home Office seem convinced that this is the right time to introduce identity cards because, in their opinion, the advances in technology have been significant in the past few years. Assuming that you are presented with a proper business plan (that is, you know the Home Office's requirements) do you think that belief in the technology is correct?
Mr Birch: Setting aside my deep-seated objection to the use of the word "business plan" in this context, because the Home Office is not a business—I am sorry, that is just a hobbyhorse of mine—I think the answer is yes. In other words, if Parliament were to articulate a particular set of requirements of what they wanted from a national identity management scheme, from the technical side I would say that actually I do not have any fundamental concerns about the ability of the technology to implement the solution. I am perfectly confident about it, in fact.

Q502 Dr Iddon: Does anybody dissent from that view?

Mr Fishenden: I think it goes back to the question of what the intended outcomes are. I would certainly make the key point that technology is there to assist. I would not see the use of biometrics, for example, as meaning that you could take away a lot of the human element, the face-to-face, which the technology should be supporting rather than being seen as a replacement. But if you go back to some of the stated purposes of the card as they exist at the moment, which are to tackle ID fraud and the like, the biggest growth is around online and digital identity fraud and phishing attacks and the like, and yet I have heard nothing in any of the consultation about how this card would operate in an online context. I know Ian Watmore and others have said that potentially it could be used for online public services, through things like the Government Gateway, so that you could get to local council and central government services, but there has been no discussion about what that actually means for the user with an ID card. If we go back to how is it going to tackle the largest growth area of identity fraud, which is online, I am not clear how in the domestic environment, for example, biometrics are going to be used. Are we back just to chip-and-pin type technology? In which case, if that is the main use of it, it is without biometrics, so is the debate about biometrics a bit of a side issue in that context for most of the typical daily scenarios in which people could actually be using the card?
Mr Birch: I am sure it is only a matter of time before you get an email in your inbox saying: "Hello. This is the Government. We are just testing our new identity system."
Mr Fishenden: Click here to get your ID card.
Mr Birch: "Please type in your date of birth . . ."

Q503 Chairman: That is very cynical.
Mr Birch: With customers of the banks, it happens all the time.
Professor Thomas: There is a really key point here because the e-government agenda is trying to move to online remote access and yet it is not clear that the national identity register helps you to identify people when you are interacting with them online. If you are simply relying on chip and pin technology and not on the biometrics, then the card can be stolen and the pin can be stolen or the card can be broken and forged—and it will be a lucrative target, so there will be plenty of resources going into doing that. If the biometrics are being checked remotely, then the remote biometrics, as a digital stream, can be captured and compromised. You can envisage man-in-the-middle attacks and various other classic security attacks which would mean that somebody's biometrics could be presented as if they had been read at that moment remotely, when in fact they had been captured some time previously and stored. That raises, as I said earlier, the horrifying prospect that individuals will simply be barred for life from accessing certain services because their biometrics have been compromised, they have been stolen, and there is no way of changing them. It is a serious error of system design to use something that cannot be changed as an authentication mechanism, under circumstances where that something, that cannot be changed, could be compromised.

Q504 Dr Iddon: Professor Thomas, is the technology available to get around all the problems that you are presenting to us this morning?
Professor Thomas: Some of them are inherent in the structure of the requirements. Technology is not magic. It may look like it sometimes, but when you have requirements that genuinely conflict then there is genuinely no solution to them other than to modify the requirements to a set that do not conflict. That is why it is so important to really look at the requirements and analyse them for potential conflicts.

Q505 Dr Iddon: Let me move to another subject. This is such a massive scheme, complex as we are hearing this morning, is it possible to trial the scheme and roll it out gradually across the country or does it have to be all or nothing?
Mr Kalisperas: It needs to be the former. It needs to be piloted and then rolled out gradually. If there is one lesson that has already been learned by the Government on IT projects, it is that "Big bang" does not work.

Q506 Dr Iddon: Would that be the agreement of all the panel, that we should trial it, pilot it, whatever the word is, before rolling it out across the country?
Professor Thomas: Yes. But I would add that the purpose of that would be to discover the weaknesses, the things that had gone wrong, and therefore you would need to allow plenty of time and plenty of budget for backtracking, for making modifications, perhaps for radical revisions of the scheme.
Mr Birch: I would trial it. Obviously you need to do these things in a phased way. Personally, I would do that slightly differently, because it is what you are piloting, so you would not issue ID cards to everybody in Manchester and see how it goes. It does not make any sense to do it like that. Most of the benefits that have been put forward as part of the consultation process are benefits of people simply having an identity number. My suggestion would be that, in the first instance, you simply pilot giving everybody an identity number; in the second phase, you pilot linking those identity numbers to them through some form of biometric register; and, in the third phase, you pilot the use of the card to delivery government services using that number. What needs piloting is giving everybody an ID number, not building a gigantic database and populating it.

Q507 Dr Iddon: We have already broached the topic of risk
Mr Birch: Yes, there is a risk of me repeating myself!

Q508 Dr Iddon: And various of you have already outlined some of the risks you see associated with this project. Do you wish to expand on that? Do you want to give us a definitive list of risks we need to look out for?

Mr Birch: First, as the backstop, the risk of not having some form of national identity management system is quite large, because it holds us back in all sorts of other areas, not just economics. If you want to have proper online voting, more online services, e-Bay, and you do not want to be pestered to death by the bank ringing you up every five minutes: "Did you buy this telly," we need something. There is a risk to not doing anything, which is that the development of our society and economy is held back. I would just say that is my kind of bent, so the question is what additional risks are we introducing above that? I will reiterate the point that I made at the beginning—which I suppose I was slightly arguing with Martyn about—which is that, generally speaking, in technical terms, once you understand what you are trying to do, the risks are tolerable. There are gazillions of smart cards in use all around the world—you know: when I get off the plane in Brazil, my phone seems to work properly. It is obviously possible to build these things and link them all up together. The risks I do not think are really there. The risks are more the risks that we already understand from things like DVLA and so on, so the risk is that you wake up in the morning and open the paper and some clerk at the DSS has got David Beckham's record out of the register and flogged them to *The Sun* or something. That is the risk, not that some genius is going to find some way of factoring prime numbers and forging digital signatures. I am sorry to be prosaic.

Q509 Chairman: What are the risks for you?
Mr Fishenden: Going back to the earlier point, where we were talking about architecture and the Home Office aspiration not to be prescriptive, I think it would have been useful over the consultation period—which, as Nick mentioned, goes back about three and a half years—if there had been some independent analysis of the risk associated with centralised models as opposed to distributed models of tackling national identity systems, so that actually when the bids finally go in—and, presumably, if it is a non-prescriptive procurement there will be a whole variety of architectures being proposed—the Home Office would be in a well-informed position to take an informed assessment of which of those proposed models offers the best management of the associated risks. I am not aware of any work having been done over the last few years. There is certainly no openly published work from the UK Government into the risks associated with different types of technical models for national ID cards.

Q510 Adam Afriyie: To what extent has the Home Office taken advantage of learning from schemes abroad? In view of the unique nature of the Home Office scheme, what lessons could be learned or have been learned from abroad, in your view?
Mr Kalisperas: I think, in terms of who they have asked, you would probably have to ask the Home Office. I know they have had some interaction with some foreign schemes; they have looked at some foreign schemes. In terms of lessons, I think you would probably have to ask them.
Mr Birch: I am not sure all views are equivalent in this respect. Just going on some of the schemes that we have been involved in—and I think they have visited Hong Kong, for example, and that is one of the schemes that we have been involved in—how much you can learn from those I am not sure. The UK is in a very different situation. Most of the countries that are rolling out what you would call smart identity cards—modern identity cards, not just glorified buts of cardboard—are countries which already have the equivalent of the identity register. They already have some form of ID card they are upgrading, so it is not transparently obvious that the lessons you would pick up could automatically be applied in the UK. The UK, the US, Australia are examples of countries that are in a very different place with respect to identity from other countries.
Professor Thomas: I would have expected to see an analysis of the benefits that looked at countries that had identity schemes in place and did a per capita fraud comparison, that kind of thing, in order to demonstrate that there was some level of correlation between having an ID card in place and the level of serious crime, the level of terrorism, the level of money laundering and so on. I have not seen anything like that—simply assertions that the ID card scheme as proposed will provide benefits in those areas—and yet it seems to me that there are enough identity schemes around the world that it ought to be possible to do a scientific analysis of them.
Mr Birch: The requirement is not to have an ID card and whatever. The requirement is for some better form of national identity management. Looking at other cards is really only a little bit of the story, because we should be looking at other examples where modern notions of identity management appear to be helping to transform organisations and make them more efficient and responsible and so on. It is not just a question of looking at other people's cards and seeing if we want to copy the design.

Q511 Chairman: Are we being too ambitious?
Mr Birch: Personally, I think we are not being ambitious enough. I think we should be looking to a fundamentally modern, 21st century, forward-looking vision.

Q512 Chairman: Surely that is what the Government, to be fair, are saying. They are saying, "We are not going to define what is going to happen."
Professor Thomas: They have defined it, though.

Q513 Chairman: "We are going to leave it to you guys to design a system around our specification." I think you are being very harsh on the Government.
Professor Thomas: I think that is a misperception.

Q514 Chairman: I am smiling when I am saying this.
Professor Thomas: Looking at what has been done, rather than what has been said, would lead the man from Mars to assume that the real objective was to create a database of the nation's biometrics, and that

everything else was just window dressing. Because that is where all the effort has gone: into defining a biometrics database. If that is really the requirement, that is fine, the Government is entitled to have that as a requirement, but then that ought to be specified and people can focus on that. If, on the other hand, the real requirement is for a modern, societal, identity management scheme, then we ought to debate what that would look like, not how it would be implemented, and biometrics might have no part to play in that.
Mr Kalisperas: But if you seek that then you have to look beyond just the Home Office.
Mr Birch: Yes.
Professor Thomas: Absolutely.
Chairman: You have made that point.

Q515 Mr Devine: I think I know the answer to the next question, but do you think there has been a lack of open and informed debate regarding this scheme?
Professor Thomas: Yes.
Mr Kalisperas: I think there has been a fairly open debate in Parliament but I think it probably has not been the sort of debate we would like to have with the industry. It goes back to the point about a statement of the requirements and having much clearer discussion about that in particular. We have consistently said we do not think the technology is going to be the problem on this. If there is clarity in terms of the objectives, if there is clarity in terms of the business case, if there is enough time to make sure that the system is tested but there is enough time to make corrections, then I think the system will be delivered, but you need a strong customer and you need a customer who is prepared to work in partnership with the industry and to listen to what industry has to say on this. Because there is no shortage of advice and there is no shortage of willingness—and that does not come from the fact that the industry thinks it is going to make loads of money out of this, because when it comes to public sector IT projects, the industry does not make a lot of money, it gets a lot of flak—and our overriding objective for this procurement, as with all others, is to make sure that it is implemented correctly. There is enough best practice out there for government to listen and to take heed.
Mr Birch: There has been lots of debate but it has not always been terribly helpful, because ID cards carry such an emotive core to any discussion. From my perspective, as someone who is very interested in the whole area, the debate fragmented very early on. Either you were in favour of everything the Home Office wanted, in which case you were a fascist lackey of an oppressive state, or you were against it, in which case you were an anarchist: "No to ID". There was no middle ground. It just immediately went into these polarised positions. Most people, I would think, actually belong somewhere in the middle, which is: "We ought to do something about identity. We ought to improve the identity situation, but possibly what the Home Office first put forward is not quite right and deserves some reflection." I think most people are in that middle but the whole debate has been characterised by you are either for it or you are against it; you are either an anarchist or a fascist.

Q516 Mr Devine: To what extent has the Home Office communicated successfully the benefits and the risks of the technology to the public? You have made wry comments on the problems, and Jerry you made reference to the fact—as I phoned my bank yesterday and they asked me for my date of birth—that this could be on this card.

Mr Fishenden: Personally, I do not think it has been terribly well communicated, and it goes back to those scenarios. People need to understand what the impact is going to be on their daily lives. Potentially there were some quite interesting examples like proving you are over 18 to buy alcohol or to get a bus pass or whatever, but I do not think there have been enough of those in the public domain and unfortunately the few there are seem to have some inherent flaws in the way they are proposing for them to work. So communication, such as it is, is both insufficient in quantity, if you like, and the quality of it at the moment is not of the calibre I would expect.

Mr Kalisperas: Again, I think there are lessons to be learned. Citizens tend to react well to systems which have a benefit to them. So, for example, direct payment seems to have gone down relatively well because it means that the citizens are receiving their payments automatically rather than having to go to the Post Office. Again, with chip and pin, that seems to have gone down relatively well save for a couple of instances. I think the issue has been, as was said previously, mention the word identity cards and the whole debate becomes polarised, and if there was more of a link towards access to public services, entitlement, et cetera, you would get a different public response.

Q517 Adam Afriyie: I have a relatively straightforward question on costings. The Home Office has released a very precise figure, £584 million or something, for delivering the ID card scheme per year. Is that figure legitimate or lunatic?
Mr Birch: Until I see the requirements I could not comment.

Mr Kalisperas: Agreed.

Q518 Adam Afriyie: So the requirements are required?

Mr Kalisperas: Yes.

Chairman: I am sorry that has been a helter skelter through. We could have spent a lot more time on your Panel, but thank you very much indeed.

Witnesses: **Dr Tony Mansfield,** National Physical Laboratory; **Dr John Daugman,** University of Cambridge; **Dr Edgar Whitley,** London School of Economics and Political Science; and **Professor Angela Sasse,** University College London, gave evidence.

Q519 Chairman: Could I welcome our second panel to the inquiry today? I will not repeat what I said earlier but this is a key inquiry looking at the issue of the way in which Government assesses risk in terms of its policy-making, the way in which it uses scientific advice behind its policy-making, and we are very anxious to look at the process rather than, in fact, to make judgments about whether we should have ID cards or not. That is an issue for public policy. We have in front of us Dr Tony Mansfield from the National Physical Laboratory; Dr John Daugman from the University of Cambridge; Dr Edgar Whitley from the LSE, and Professor Angela Sasse from UCL. Now, before I start my line of questioning could I ask each of you, do you have any commercial interest in any of the technologies which are being proposed either by yourselves or by the Government?

Dr Mansfield: Speaking for myself I have no attachment to one technology or the other, but the area in which I work is in evaluation of biometrics, so obviously I have some interest in technology.

Dr Daugman: I do not, and I would like to correct something that was said in the previous hearing of this Committee which was I have the worldwide rights to iris scanning—

Q520 Chairman: I said that.

Dr Daugman: In fact, there are no worldwide rights to iris scanning. Anybody who could come up with an algorithm is free to deploy it. I am the inventor of the technology and the author of the algorithms that are currently used in all public deployments and I have acquired a number of patents in that, but in the year 2004 I irrevocably assigned all of my interests in those patents to a charitable trust, so I currently have no commercial, financial interest in either iris recognition or any biometric company.

Q521 Chairman: Thank you very much. Thank you for putting that on the record, and if I misquoted you I apologise.

Professor Sasse: I am in the same position as Dr Mansfield. I have no attachment to any particular technology but I work on evaluation of the technology so I work as a consultant.

Dr Whitley: No connections whatsoever.

Q522 Chairman: Thank you. It was important for me to put that on the record so that the Committee is seen to be fair in this issue. The ID cards programme team said they consulted quite widely. Do you agree, and what more could they have done?

Dr Mansfield: Well, there seems to have been a process of continual consultation and I think they have been listening since 2002, when the consultation exercise on entitlement cards was conducted. There may be one or two things that could have been done additionally. When you asked the previous panel the question one of the things which I think could have happened is better engagement between the original consultation and procurement, and there were perhaps a few opportunities that were missed for engagement with industry and academia to investigate certain solutions or certain problems prior to the procurement starting.

Q523 Chairman: But generally you are happy with the consultation. John?

Dr Daugman: Behind the scenes there has been a fair amount of scientific consultation, at least in my experience, from Home Office scientists. People have asked me specific technical questions based on the scientific literature, for example, could I point them to references. I would make a distinction between that and the public debate about ID cards which has been woefully lacking in scientific understanding. The press have picked up on all kinds of false assertions which then go on to be repeated, for example in the LSE report as fact so, as you have seen, the thrust of my written evidence to this Committee concerns the very poor quality of the public discussion of scientific issues around ID cards, but the quality of Home Office consultation in my experience has been rather high.

Q524 Chairman: We will return to some of those issues later. Professor Sasse, the general consultation?

Professor Sasse: I would agree there is a lot of consultation that has taken place and certainly I have been particularly involved in the process since 2004 when the Home Affairs Select Committee looked into the proposed legislation, and it is quite visible that they have taken on board some advice and outcomes of those consultations in the way that the proposals have been developed. However, I think it is also fair to say that possibly one of the reasons that the process went in the way that Dr Daugman just described is because right at the beginning the Home Office sought to influence the public debate in a way which has turned out not to be very helpful by basically putting out a no-holds barred, positive assertion of a whole range of benefits that could be derived from the programme, without having made a—

Q525 Chairman: A proper assessment?

Professor Sasse: Yes.

Q526 Chairman: Do you basically agree with that?

Dr Whitley: Yes. On Dr Daugman's point I know the Committee does not want to go into detail on this but we have responded to the specific allegations we have made—

Q527 Chairman: You can fight outside!

Dr Whitley: I understand, but just to say we have responded in detail to his allegations.[2]

Q528 Chairman: Tony, how reliant do you think is the Home Office upon your advice on biometrics, and what is your role in the Biometrics Expert Group? Do you have too much influence in that area?

Dr Mansfield: The Home Office draws on expertise from more than just myself. Originally there was a feasibility study for Passport Service and DVLA and Home Office about using biometrics to strengthen identity documents such as entitlement cards. The study was quite narrowly focused, and focused entirely on the biometrics component. Of course that study is four years old; the work was conducted in 2002; things have moved on since then. To my mind the Home Office has not been over-reliant on the advice that was given back in 2002–03, but it probably has not come across that way in terms of things which have been said or things which have been put out in the public arena. There is more evidence that they have considered and taken on board that has not been put on the website.

Q529 Adam Afriyie: For Professor Sasse and Dr Daugman, to what extent has the Biometrics Assurance Group been involved in the ID cards programme?

Dr Daugman: It has just begun. It had an organisational meeting in November and a subsequent meeting in February, both of which were mainly briefing opportunities for us to be briefed by Home Office officials and affiliated scientists. Things are accelerating a bit more now. We have a set of sub-committees who are investigating particular challenges looking into, for example, security and spoofing and stability in biometrics and the NIR (National Identity Register) issues, so that is just beginning now.

Q530 Adam Afriyie: So the answer is just two meetings?

Dr Daugman: So far, yes.

Q531 Adam Afriyie: And roughly how long were those meetings?

Dr Daugman: Full day meetings, or three quarters of a day, and the next is next week.

Q532 Adam Afriyie: Is your advice during those meetings given proactively, or are you reacting to probing from the Home Office?

Dr Daugman: So far we have not formally given any advice at all. We have been getting briefs.

[2] The LSE Identity Project Response to Dr Daugman's submission is available at http://is2.lse.ac.uk/IDcard/default.htm

Q533 Chairman: Angela, could you comment on that?

Professor Sasse: This is correct. Also, I raised some questions in the briefing and they were followed up by the relevant members of the ID cards team who asked my advice on the trial they are planning starting towards the end of the year, so they did actually consult me subsequently on some of the points I raised.

Q534 Chairman: Could I ask John and Edgar briefly, John in particular, given your involvement with iris scanning and the history you have with that, how can you be independent?

Dr Daugman: I am an academic; I have been at Cambridge University for about 15 years since 1991; can intellectual work which has practical applications be deemed independent? I think so. Overall there are broad mathematical issues in decision-making under uncertainty, pattern recognition, fusion of evidence—all kinds of abstract questions about how you make decisions about someone's identity perhaps by searching a database the size of the entire country based on some biological data. Those are fundamental scientific and mathematical questions about which I have a lot to say, but having no financial interest in the technology I think I can claim independence. I will admit to an intellectual and scientific interest in the technology but no financial interest.

Q535 Chairman: Would you agree? In terms of the independence of the advice of governments, that is the questions I am trying to get at.

Dr Whitley: I think the raw scientific evidence such as, for example, was given in the supplementary evidence from the Home Office, we are not actually on that great a disagreement with. We both said that the number of real trials—the figures are here—for fingerprint trials the database sizes were in the millions, face recognitions in the tens of thousands and iris performance statistics from independent tests were limited to the hundreds. If that is the scientific evidence we have no disagreement with it. It is a question of, on the basis of that can you roll out biometric identification in the time scales and at the cost levels that the Home Office is intending. That is where much of the disagreement arises.

Chairman: We will return to that. Margaret?

Q536 Margaret Moran: We heard in the last session and, indeed, elsewhere that there seems to be a lack of clarity about aims and uses of the scheme. Would you agree with that?

Dr Whitley: Yes.

Professor Sasse: Yes.

Dr Daugman: No.

Dr Mansfield: Partly! There are some uses that I think are quite well specified. To the use of biometrics, for example, at the time of enrolment for an identity card to ensure that someone has not previously registered for an ID card using completely different identity details, that is reasonably well established so there is a fair bit of clarity there. Some of the other potential uses are less clear, but when we are talking about an identity management system for the future it is difficult to predict exactly everything which could be done in the future. That is why part of the uses are well-defined and some are not so well-defined.

Dr Whitley: To give two quick illustrations, the first came out in the press a couple of weeks ago where Mr Burnham was saying it would be a good idea to have health information stored on the central database;[3] Mr Clark, responding to Simon Carr[4] said, and repeating what had been said in Parliament, health information will not be part of the database and will require primary legislation to introduce it. Now, if you are thinking of introducing that you had better get that down in the specifications for your system quickly, rather than five years down the line introducing a voluntary database that requires storage, processing, et cetera, et cetera. It is those kinds of things that certainly give me concern about the clarity within the system. Similarly on biometrics v PIN numbers. Mr Burnham said biometrics is great for assessing identity; other forms of authentication, such as PIN numbers and passwords, can be stolen along with a card so are much weaker at linking a person to an identity.[5] Again, the Government's scheme seems to be for large parts using PIN numbers to verify that this is your card, a point that was made earlier.

Q537 Margaret Moran: We have been told in evidence that the technological architecture of the scheme is dependent on the business requirement. Do you agree with that, and you can give short answers.

Dr Whitley: Again, it is not clear exactly what the business requirements are. There are Home Office business requirements but all the other government departments who are expected to link in have not yet got round to doing in detail what kinds of services, and whether it is cost beneficial for them to link into the system, et cetera.

[3] *The Sunday Times*, April 23, 2006 "Labour U-turn over ID card medical details" available at http://www.timesonline.co.uk/article/0,,2087-2147744.html

[4] Available at http://press.homeoffice.gov.uk/Speeches/hs-letter-simon-carr?version=1

[5] Answer to Parliamentary question 4167 19 July 2005.

Professor Sasse: One of the benefits that the Government keeps returning to is that it would reduce benefit fraud. Now, if you look at the Department of Work and Pensions' statistics about how benefit fraud is committed you will find that well over 90% is committed by people who do not lie about their identity. They are perfectly honest about who they are; they lie about their circumstances. So, that said, you would need a much more detailed proposal. Now, a strong identity might allow you to pick up more easily if somebody has several jobs or claims they cannot work, but you would need a much more detailed proposal to see how establishing a strong identity would help you to realise that promise.

Dr Daugman: Certainly the technology architecture depends on the goals which are set. I am not sure I understand what is meant by the business architecture. If it means, for example, federated versus centralised databases then clearly that is an architectural issue.

Q538 Margaret Moran: Has the Home Office communicated clearly throughout all the phases of this project?

Dr Daugman: You mean publicly or privately?

Q539 Margaret Moran: Both.

Dr Daugman: Obviously privately we would not, in general, know the answer to that. In my personal experience, yes. Publicly I would say it has been less successful.

Dr Mansfield: I would agree. Given that there can be so many misconceptions about how the scheme should work, would work, there are some problems with communication.

Dr Turner: There seems to be a magical assumption that somehow the use of three biometrics will produce the result that no one has ever achieved before. Do you think three biometrics are necessary? Do you think that maybe in hitching the wagon to three biometrics we are setting up such complications for ourselves that the scheme may fall under the weight of its own over ambition?

Q540 Chairman: Is it achievable, as well?

Dr Mansfield: The different biometrics are kind of there for different purposes. I think if we have an identity document we would want it to look like a traditional identity document and, indeed, to be used as a passport within Europe. That implies it should have a photo on it which means you are collecting face biometrics. Also so you may be using finger prints as a primary biometric to establish a unique identity. Moreover, you may want a third biometric so that citizens that have an identity card, a wide variety of citizens, are able to biometrically prove their identity. If some people have difficulty finger printing, they can use iris instead. The fact

there are three biometrics does not necessarily mean they have to be fused in a very complicated way and add a lot to the complexity of the scheme. Some of the things are there quite naturally; some are there to give an element of choice.

Dr Daugman: The role of substitution opportunity is clear; some people may lack eyes or fingers. The fusion is a much more subtle issue because, if you combine a strong biometric with a weak one, for example, the face is a very weak biometric, in a certain sense you can end up with a performance that is intermediate between the two—in other words, averaged, in other words, inferior to what you would end up with had you used only the stronger biometric. Now, there are ways to fuse stronger and weaker biometrics to improve performance, that is a subtle mathematical point, but I believe as currently expressed the goals of the Home Office do not contemplate fusion but more substitution.

Q541 Dr Turner: Is that absolutely clear, that fusion is not involved?

Dr Daugman: I have seen correspondence from Katherine Courtney to that effect. For example, iris has the unique ability to make vast database searches without making false matches, but it is not necessarily the easiest to use. Face in a sense is the easiest thing to present; it is just not very discriminating; so to search for detection of multiple identities in the clean, new database register would be the main role for iris, not every time you want to use a credit card. You see, if you combine biometrics at decision level in a certain sense you are using either an "or" rule or an "and" rule. The "or" rule says you should pass either of my tests. In that case the false match rate gets worse; the false reject rate gets better. The "and" rule says you must pass both my tests. In that case the false match rate gets better, and the false reject rate gets worse. So there are subtleties about the two different types of errors that can be made in the biometrics and the desiderata of fusion schemes.

Q542 Chairman: Do you basically agree, both of you, with that assessment?

Dr Whitley: In terms of what?

Q543 Chairman: That (a) we are not looking for fusion, and to be fair the Government has not said it is going to have huge technologies, but we are looking for three biometrics which give you alternatives within the recognition system.

Dr Whitley: Except of course that if you are going to be using biometrics at the front line rather than for enrolment then saying you are going to have either finger prints or iris—probably not face—for a reasonable security risk, then that means you are going to have to have two different sets of readers which, again, has cost implications and practicality implications.

Professor Sasse: For the individual it does have implications. If you have to enrol on three biometrics rather than one the enrolment time goes up. Also potentially I have seen in the past that particularly people who do not use the systems frequently easily get confused between face recognition and the iris system and they end up presenting their face to the iris system and vice versa.

Q544 Dr Iddon: John Daugman, iris recognition is controversial, is it not?

Dr Daugman: I do not think it is particularly controversial, no. There is a lot of misunderstanding about the eye. A typical argument against iris recognition goes as follows: the iris is part of the eye; the retina is also part of the eye; oh, look, here are some conditions and diseases that may affect the retina, therefore iris recognition will not work. That was the general thrust of the LSE objection to the scientific feasibility of the iris biometric, so clearly that is based just on an elementary misunderstanding about the parts of the eye. For example, cataracts affect the lens of the eye which is behind the iris and in front of the retina, so cloudiness of the lens and cataract would interfere with retinal imaging but certainly not iris imaging. That was one of several such elementary misstatements of fact that occurred in the LSE report and in the public and in the media.

Q545 Dr Iddon: What about biological changes in women, for example?

Dr Daugman: Yes. MPs have made a number of groundless statements, for example, that women who are menstruating cannot use iris recognition.

Q546 Chairman: Excuse me, John. We made that assertion because we heard evidence in the US to that effect. It was not something that MPs made up. It was on the basis of evidence which we had in the US.

Dr Daugman: I would love to know the nature of that evidence. I do not know what model of menstruation involves the iris. Likewise there are assertions that looking at an iris camera will give you an epileptic fit. These are speculations which have a history of rising in their credibility because what is introduced as a speculation in one report, or document, including US Government documents and the GAO report, become promoted to the status of facts in the next report, and—

Q547 Dr Iddon: Are you saying there is no scientific evidence for these biological changes? When a woman becomes pregnant, for example. It is not just menstruation.

Dr Daugman: I have done considerable investigation into this question over the last 10 years, the question does the iris change, and there is a lot of history I can tell you out there. There is currently no scientific evidence that I am aware of that supports the view

that the iris changes over time. Now, there is a cult practice called iridology which is similar to palm reading, it claims to be able to assess the state of health of each organ in your body as well as assess your personality and your interpersonal compatibilities and, indeed, predict your future. That is, of course, hocus pocus and there are six or seven published scientific studies by medical groups that bothered to try to take it seriously and do double blind studies, and their articles are published in journals like the *British Medical Journal* and the *Journal of the American Medical Association* with titles like *Looking for Gall Bladder Disease in a Patient's Iris*.

Professor Sasse: My title is Professor of Human-Centred Technology so if people are concerned about some of these issues then I will just turn around and basically say that there is no scientific evidence; it is hocus pocus, and dismiss it. In some parts of Europe there are parts of the medical establishment and there are certainly lots of people who believe in alternative medicine and found that it has helped them. Therefore, there are, of course, concerns basically that, if their iris image is stored in a database that the Government has access to, this might have implications, say, for medical treatment you can get or being selected or omitted from certain jobs, or whatever. I think it is quite hard, and not right to just go and dismiss these things. There is more of a process that has to take place. Similarly, I have spoken to some doctors who basically say that they can see changes in the iris. I cannot say they are right or wrong, but there definitely is a belief and it is not useful to dismiss these things out of hand. The other point is this confusion between the retina and the iris, which is something that is confused by the general public. Quite forgivable because they are both called a scan even though they are quite different technologies, and what the user sees is this light beam coming out of it, and they get confused and think their eye is being scanned, when all that happens is this beam illuminates the iris to make sure you take a good enough photograph. But I think the manufacturers of these systems do themselves a disservice by calling it a scan which keeps furthering this misconception between the two.

Dr Mansfield: We have run evaluations of biometric technology and we have not observed any such thing with menstruating women or whatever, so it is unlikely to be a direct cause and effect. There may be other issues which are associated with a particular person which meant they had difficulty in using a particular iris scanner, or were in a bad mood and would not co-operate on a certain date, or whatever. So there is no reason why iris recognition technology should have such an effect.

Chairman: It would not affect MPs!

Q548 Dr Iddon: Tony, you said facial recognition was not a feasible option, yet the Home Office appears to be pursuing this line of inquiry. Why?

Dr Mansfield: We said face recognition was not a feasible option for identifying one person in the national population, and that is fairly obvious when you consider identical twins, where one would appear very similar to another. But if you have a passport you are expected to have a face image on the passport to meet with international requirements, if your passport is going to be usable. Therefore, it is natural that faces would be collected and would be one of the biometrics within an identity card scheme.

Q549 Dr Iddon: Angela, we have not mentioned so far this morning the societal impact of any scheme that might be introduced with identity cards. Do you think the Home Office has done any or even sufficient research on the societal impact of an ID scheme?

Professor Sasse: I think they did become aware of the issue during the Home Affairs Select Committee investigation. There were basically several submissions that pointed out that there is a certain part of society where people have complicated lives, that there are people who could not very easily go to enrolment centres and so on, so, yes, they certainly did start to engage with that issue. I am not sure that really in every detail the impact on various individuals in society has been considered thoroughly enough.

Dr Whitley: I have just a quick illustration. At the Westminster e-Forum meeting on 14 February there was a speaker from a mental health charity[6] pointing out that if you have mental health problems and schizophrenia[7] and are concerned about government, being forced to enrol in a government-controlled database is clearly not going to be very beneficial for you.

Q550 Dr Iddon: So what do we do about this?

Professor Sasse: Similarly another example is that doing the UKPS trial it became quite clear that certain groups of disabled people have significant problems with some of the technology, but I have just been approached, for instance, by the RNIB who say that from this report they cannot work out what exactly the reasons for it are and yet this charity, for instance, is not able to investigate in more detail exactly what the problems are and how the systems should be developed. So there is a bit of a lack of depth and a lack of following-up on problems that have been discovered to see how they could be overcome.

Q551 Dr Iddon: So is anybody pursuing any research in this?

[6] Jane Harris, Senior Campaign Officer, Rethink. Presentation in Westminster eForum "Implementing ID Cards" report, ISBN 1-905029-31-4.

[7] *Note by the witness*: I misspoke here; I meant "paranoia", rather than "schizophrenia".

Dr Mansfield: From my current involvement with the ID cards programme, I am aware that some of these problems are being followed up.

Q552 Chairman: By whom?
Dr Mansfield: By the Home Office.

Dr Daugman: I am working with three ophthalmology groups investigating those questions about whether individuals who have visual impairments have difficulty with iris recognition. Those are the RNIB, the Manchester Eye Hospital and the Edinburgh Eye Hospital. I have arranged for equipment to be made available to them so they can conduct that research.

Q553 Dr Turner: Can you give me your views, please, on the risks involved in this project, and do you think that the Home Office has considered them seriously enough?

Dr Mansfield: In 2003 I was at a risk workshop[8] at an early stage looking to try and identify the risks and possible mitigations. It is certainly well aware of the risks and is identifying and trying to manage risks. The risks I would say are probably because it is a very large project, a very large procurement, of which biometrics is just one small part. There seems to have been a focus on the biometric element as being the most technical and perhaps least understood element of the whole scheme, and to my mind assuming that is where all the risks lie is totally incorrect.

Dr Daugman: In April of 2004, about two years ago, an important study called *The Challenges of Complex IT Systems* was published by the Royal Academy of Engineering in co-operation with the British Computer Society. That is a substantial document that tries to understand both why complex IT systems have in the past sometimes failed and it also charts the progress internationally of the failure rates, which have improved quite a lot in 10 years. That document, together with other significant documents on risk assessment, is a big part of the brief that has been given to the members of the Biometric Assurance Group.

Q554 Dr Turner: Presumably there has to be a risk that biometric data can be falsified, or at least stolen and attributed to the wrong person, especially if a successful potential hijacker, for instance, were to hack into the database. How certain can any of you be that those highly dangerous risks cannot happen?

Dr Daugman: CESG within GCHQ have a substantial research programme in this area. I am assisting them in assessing the security risk. You have to distinguish between two kinds of replay attacks; the digital one, which involves hacking into the database, trying to steal or decrypt a secret part of the database, and the other is an analogue replay attack by putting on a latex gummy finger print, for example. Those have different counter measures associated with them. Briefly, the risk of digital replay attacks are essentially those of cryptographic code-breaking, so they have encryption protocols which have been well established for decades now, particularly DES3. Those are certainly no greater than the risks of security communication, and incidentally with some biometrics you can permute the bits, or the bytes, of the data so that a given stored iris code has no value tomorrow or next month, or indeed one minute from now, because there are 10 to the 507th power different permutations of the data, provided that the same permutation protocol is followed at the hosts, as at the database. Essentially an iris code as a digital set of data becomes of no value, if it is stolen, it has no value after the next permutation. I would say there is greater vulnerability, substantially, to analogue replay attacks, for example, wearing a contact lens which has somebody else's iris pattern printed onto it, either for concealing your own identity or impersonating another identity. I regard that risk as probably the weakest point of that particular biometric. There are eight or 10 physical methods as well as software methods that have been developed to detect false patterns on the surface of the eye as opposed to the iris pattern. The true iris lies inside the eye; the pupil is always moving; the iris pattern is stretching as the pupil moves—there are six or eight physiological as well as other photonic counter measures but most of those are unproven, they are assertions of principle, and that is going to be one of the main elements of testing and assessment in the forthcoming year.

Professor Sasse: There are a lot of different ways of attacking a system and it might be quite difficult to mount such a technical attack but, on the other hand, bribing somebody to store my biometrics against a different name is fairly straightforward, so what you have to do is the entire socio-technical system. That is, the identity card system has to be engineered and operated to an extremely high standard, not just of technical assurance but also of behaviour and monitoring and auditing of all the interactions that take place with a system. The problems that have happened in the past are simply because the wrong person's name has been entered against the wrong biometric. There have been several cases of false arrests in the US, and you may remember the Brendan Mayfield case, so these kind of things happen and I think you have to consider there are many different ways of how you could try and attack and misuse the identity in a system, and that it is quite a complex exercise. I think any security professional will tell you that you cannot guarantee that a particular risk will actually happen; all you can do is mitigate the risk to the degree of the resources you have available to do it.

Q555 Chairman: Do you agree with that?

Dr Whitley: Yes. In terms of the risk it is broader. There is a very practical risk that the IPS is only piloting the recording of fingerprints from late

[8] *Note by the witness*: Entitlement Cards Risk Workshop, 6 March 2003, Home Office.

2007[9], and the scheme is supposed to be up and running in 2008/2009. If that piloting reveals more problems than the roll-out scale that they are talking about, and I think they are talking about up to 50,000 enrolments a day, so if there are any practical problems there are risks there. There are the security risks, the lack of specifications, the central database rather than a distributed one, all those kinds of things, and there is also the risk that Ministers seem to be want to be rushing the scheme for political reasons. They want enough people to be on the scheme so if they do not win the next election the Conservatives will have a much more difficult case for cancelling the project[10]. And, again, rushing projects makes things go wrong.

Q556 Adam Afriyie: In the US, United Arab Emirates, Hong Kong, Philippines and Belgium, I think, there are various different ID card models. To your knowledge, has the Home Office investigated these various international models and, if so, have they learned the lessons that other nations have learned?

Professor Sasse: Yes. I think they have taken great effort to look at other schemes that are in operation and to learn as much as possible from them. However, as a scientist I have a slight problem with some of that in that in several of these schemes there are no proper controlled observations available, so what we will be getting is a statement from the Government saying, "We will give you the exact figures for the UAE. They have operated these schemes for these persons, they have made so many successful arrests", and they will claim that no person in the database has managed to enter the United Arab Emirates. Now, if you managed to beat that iris scanner and managed to get into the United Arab Emirates—it is a claim that is very difficult to verify! There have been no observed, properly controlled trials where we would have the figures that we can work on. We basically have to take on trust what they are saying. Also, what you have to consider is that systems operate in a particular social and cultural context, and the social and cultural context in those countries may not be exactly the same as in the United Kingdom, so certain behaviour that might be required from the citizen user in order to make the systems operate that may be perfectly acceptable there may not be acceptable to the citizens of the United Kingdom, and that aspect has not been looked at in a great amount of detail.

Q557 Adam Afriyie: My experience echoes yours. I was in Dubai recently and I did not see any piece of equipment anywhere scanning anything—

Dr Daugman: That is because you did not require a visa to enter. It is only for foreign nationals who require a visa who are submitted to the iris camera. And, by the way, about 1 million iris codes have been enrolled in that deployment, and about 8 million in Andhra Pradesh in India in a welfare scheme, so the total number of iris enrolments is now around 10 million—

Dr Whitley: I was simply quoting from the Home Office submission. That is all.

Q558 Chairman: But the point Angela was making is it is hard to verify the effectiveness of these schemes.

Dr Mansfield: In the schemes which are operating somewhere else using biometrics one of the things we know is that the environment, the population that is using the system, have a strong influence on the performance and the way these systems will work, so it does not matter how closely we look at other large schemes; it does not necessarily tell us exactly what would happen with biometrics on the United Kingdom scheme and, as Angela pointed out, the operational data is not quite the same as data in cold circumstances so one has to interpret what one finds out.

Q559 Mr Devine: I think I know the answer to this but has there been a lack of open, informed debate regarding this scheme amongst the public?

Dr Daugman: I think I have answered that!

Dr Mansfield: It is open but not terribly well informed.

Professor Sasse: Yes.

Dr Whitley: Yes.

Q560 Mr Devine: Do you agree with the evidence we have received which says the public discussion of scientific issues, both social and technological, relating to identity cards has been of poor standard?

Dr Mansfield: Yes.

Dr Daugman: I am the author of that sentence, so of course!

Professor Sasse: It has been of a poor standard but I would have to take issue with the author. With all the respect I have for Dr Daugman, I would say this is not something that can be pinned on the LSE. I think the Home Office itself, in my view, was guilty of this by basically, when they started their first opinion polls on the matter, putting forward this agenda of things that would be fixed through the introduction of an ID card without any clear analysis, and I think they were quite cynically pushing certain buttons they knew would work—illegal immigration, organised crime, terrorism—and basically promising, "If we introduce the ID card it is going to deal with all of these problems."

[9] Page 31 of PDF of UKIPS Corporate Plan 2006–16 available at http://www.passport.gov.uk/downloads/IPS—Corporate—Plans06.pd

[10] Jean Eaglesham and Maija Palmer, "Labour races to introduce ID cards", *Financial Times*, April 17 2006.

Q561 Chairman: In terms of the public debate surely the LSE report, which you were both involved with, has dominated much of the public debate. Has that been a good thing or not?

Dr Whitley: It certainly has informed much of the debate. Do not forget—

Q562 Chairman: With heat or light?

Dr Whitley: Hopefully with useful contribution! It is a 300-page report. Just as one aside, it is portrayed as being this completely off-the-wall, completely bizarre set of results. We had a look at the conclusions of the Home Affairs Select Committee and the conclusions of our own report, and 71 out of 94[11] of those conclusions we either strongly support or conditionally support, so it is not as though we are saying strange things; we are just presenting different sides to the argument. The glass is half empty rather than half full.

Q563 Chairman: Angela, do you remain faithful to the report?

Professor Sasse: I do not agree with every single detailed point in it but it was a valuable contribution and I have been quite astonished by the way in which the Home Office reacted against the report because the intention was to seek a constructive debate and unfortunately it did not quite work that way.

Dr Whitley: More generally, I think the way the Home Office reacted to the LSE report has very worrying implications for the way independent academic advice is presented in the future. The kinds of abuse we have received, ad hominem attacks from Home Office ministers, from the Prime Minister all the way down, is going to make academics very reluctant to stick their heads above the parapet and say, "I think Government is not right in this", or that there are different opinions that need to be taken into consideration.

Q564 Mr Devine: Do any of you think this can be rolled out in 2009, considering we are now halfway through 2006?

Dr Whitley: I have real doubts that it will roll-out successfully in that timescale unless either costs are increased or significant compromises are made about the implementation of the system.

Q565 Chairman: Would you all agree to that?

Professor Sasse: A lot will depend on the next trial that is being planned.

Dr Mansfield: I cannot say that the Home Office have particularly said, "It will roll out in 2009 no matter what." There is a lot of water to go under the bridge in terms of what happens during procurement, what happens in terms of trials, what happens in terms of roll-out activities, so time will tell.

Q566 Chairman: John, do you support that?

Dr Daugman: Yes.

Q567 Adam Afriyie: So we would not bet our salaries on the project being delivered on time. Can I offer another wager? Would you bet that the estimates of cost from the Home Office will be met?

Dr Daugman: Which are the—

Q568 Adam Afriyie: The £584 million a year.

Dr Daugman: Well, I am sure the cost will lie somewhere between that and the £19 billion that the LSE estimated.

Q569 Adam Afriyie: It is not a spread bet!

Dr Daugman: The roll-out is quite incremental and phased over three or four years. I have seen 2008 and 2011 with a gradual attachment to passports, so it is not a D-day event.

Q570 Adam Afriyie: Is everybody else happy with the Home Office costing of the project?

Professor Sasse: We have not been given enough detail to really check the validity.

Dr Whitley: To be absolutely clear the £584 million is the average annual running costs to the Home Office alone, not the set-up costs and not the costs to other departments. On the basis of no technology trials or limited technology trials and specifications still being changed I just cannot see how they can be so clear that it is £584 million. I think Mr Clarke said it might actually go down[12] and Mr Burnham said that despite a year from that initial figure being released and more information being gathered, overall the figure has not changed.[13] I cannot see how that figure can stand in the future. And, just for the record, the £19 billion was our upper limit. We provided three sets of estimates, low, medium and high, and the £19 billion is the high limit of a worse case scenario, where lots and lots of things do not succeed in the way the Home Office would expect.

Q571 Dr Iddon: This morning we have seen "If this, if that". How on earth can you even stab at £10.6 billion or £19.2 billion when you do not know what the Government's intentions are?

Dr Whitley: We provided detailed appendices where we go through a whole series of line items for the kinds of things we expect based on the architecture as was made publicly available in various Home Office documents, so it is our best guess based on very limited information.

[11] *Note by the witness:* I misspoke here; the actual figures are 79 out of 91.

[12] HC Deb, 13 February 2006, Col 1119.

[13] HC Deb, 27 February 2006, Col 90W.

Q572 Dr Iddon: But has it not been irresponsible because it has thrown the debate against identity cards? Was it not irresponsible to stab at such a high figure when you have not got the evidence to support that figure?

Dr Whitley: We provided three figures, a low, a medium and a high, based on our assessment of the likely cost elements of that. If it is irresponsible to introduce to the debate that there might be other ways and other things that need to be taken into consideration, I do not see it as being irresponsible.

Dr Iddon: It has thrown the debate against the ID cards in a lot of circles, that is the problem.

Chairman: I am going to leave that line of questions but I would like to bring Brian back to a question we missed about the technology trials.

Q573 Dr Iddon: In March, Tony, you wrote: "All systems need improvement". What exactly did you mean when you wrote that?

Dr Mansfield: This was in the context of the report I did reviewing the UKPS trials last year. The UKPS ran a pilot; the pilot was mainly looking at the process issues and user issues in enrolling people for the three biometrics, iris, finger print and face recognition, and the performance figures that were obtained were not terribly good for those technologies mainly because of the nature of the trial. The trial was not devised as a performance trial but it illustrated that if you just buy off-the-shelf systems and deploy them with no adaptation to the ID cards programme the performance would not be terribly good, so my comment there is to say that if the results had been reported then there should be a recommendation that there needs to be improvements to the technologies, because clearly the performance was inadequate in that trial.

Q574 Dr Iddon: So what trials are you believing are necessary now? What would you recommend the Home Office to trial, and how?

Dr Mansfield: The kind of trial that I would like, and it probably goes back to earlier than that particular report, back to the Feasibility Study 2003, would be some trial where the Government or the Home Office is working with industry to try and deliver the best possible performance and address the performance issues that get identified in some of these larger trials, for example, the issue with people with disabilities.

Chairman: Thank you very much indeed for an interesting session.

Wednesday 14 June 2006

Members present:

Mr Phil Willis, in the Chair

Adam Afriyie	Margaret Moran
Mr Robert Flello	Mr Brooks Newmark
Dr Evan Harris	Bob Spink
Dr Brian Iddon	Dr Desmond Turner

Witnesses: **Joan Ryan,** a Member of the House, Parliamentary Under-Secretary of State for nationality, citizenship and immigration, and **Mr Vernon Coaker,** a Member of the House, Parliamentary Under-Secretary of State for policing, security and community safety, gave evidence.

Q1142 Chairman: Good morning to our two ministers, Joan Ryan and Vernon Coaker. Welcome to this our final evidence session on two of our case studies on ID cards and the classification of illegal drugs. For your benefit and the benefit of visitors this morning, this is part of an overarching inquiry looking at how scientific evidence informs government policy, how it informs risk, and how Government takes advice from an evidence base and a scientific base. That is its purpose. Our job is not to decide whether ID cards are a good thing or a bad thing. It is very much a matter of looking at the science behind it, the evidence behind the Government's policy. We are, first, going to run through the issues on ID cards and then move on to drug classification. Several witnesses have said that they were unclear about the objectives of the ID card programme. Are you clear what they are? Would you give us a quick canter through that?
Joan Ryan: Yes, I think I am. I am happy to do that. The reason I am clearer than most is because I served on both the standing committees that took ID cards through the process in the Commons. I would outline four main reasons for ID cards. That is not to say there are not or will not be others as this develops but I think we have four key objectives. The first I would identify as being to enable people to have a secure means to establish and protect their identity. The second is to help to counter illegal immigration and work to strengthen our borders. The third is to counter the misuse of public services, to ensure that public services are used by those entitled to use them, and therefore also to improve efficiency and effectiveness in service delivery. I would identify the fourth as to counter organised crime and terrorism, to disrupt the activities of terrorists and organised criminals, and to make the UK the most difficult place in the world to use false identity.

Q1143 Chairman: Do you feel that from the beginning of this process the Government has been clear as to what its objectives are since David Blunkett announced them as the Secretary of State a good number of years ago now? Do you think there has been a clear timetable and are you working to that timetable? Are you conscious of a timetable?
Joan Ryan: I do think the Government has been clear right from the beginning and, as I say, I have had quite some involvement in that process from an early stage. I think we were very clear on the face of the Bill. We have been clear in the early discussions and consultations that took place. These four reasons have figured throughout. It is true that people have sometimes given them in a different order and perhaps with a different emphasis.

Q1144 Chairman: You are working to a timetable?
Joan Ryan: In terms of a timetable, we have what I would describe as a broad timetable with landmarks along it, rather than a detailed timetable. If we go back to David Blunkett in 2002, we can see the progression; we can see that a very big landmark was getting the legislation enacted. There was a delay there of a year. That is now part of the timetable. In the main, we are now at a stage where we are seeking to move to procurement and the procurement process itself will have a very big influence on determining the timetable from the point at which procurement happens.

Q1145 Chairman: As the Minister responsible, are you now clear in your mind that, from now until the time that we all have ID cards, not only is the timetable mapped out but there are no hurdles that are yet to be overcome and, if there are any, what are they? Is it all plain sailing?
Joan Ryan: On the timetable, we do not have a date at which I can say to you, "Here you are. On this date the scheme will be ready and we will start at that point rolling it out". I can tell you where we hope to be. However, as I have said, the procurement phase is crucial. We have landmarks in this timetable to work with our partners to deliver on our building blocks. The committee is probably aware of things like biometric passports, UK biometric visas and biometric residents' permits. Those kinds of developments and the feedback from them will help determine the timetable. The reason why the timetable is perhaps a bit looser than what might be called a very detailed timetable is because of that development and because we want to be very cautious on the basis of all the lessons we have learnt from good and bad projects.

Q1146 Chairman: You are giving the impression that there are no problems facing you at the moment, no scientific problems facing you at the moment, and all has been resolved.

Joan Ryan: I am not attempting to give that impression, Chairman. What I am saying is that the procurement phase is going to be absolutely crucial and trialling during that procurement phase in identifying for us where the issues are, if problems are going to have to be caught. It is because we are taking it in that incremental developmental way that we expect therefore to be able to deal with issues as they come up in that procurement.

Q1147 Chairman: Has procurement begun already?
Joan Ryan: No. We have done a preliminary information notice.

Q1148 Chairman: Has that thrown up any problems?
Joan Ryan: That has obviously alerted the market to the fact that we are seeking to go forward towards procurement. We have done some very detailed market soundings. What we have identified through this are risks rather than problems. De-risking is a very important part of the way we are going forward and of the incremental build with the building blocks I have mentioned and also the way in which we are hoping to structure procurement.

Q1149 Mr Flello: Do you think that perhaps some of the confusion and difficulty has arisen because actually as the whole idea around ID cards has evolved, more and more really good uses are being thought of for them, for example, in terms of employment? If somebody is coming to an employer and needs to prove their identity, ID cards would be a very good mechanism in that sense. Do you think that some of the confusion and difficulties have arisen simply because there are so many add-on benefits for an ID card?
Joan Ryan: I think that is exactly right. There are a number of other schemes in different countries around the world, all of which we are looking at and we are talking to the people involved. I know the committee has had some evidence on some of these issues and our conversations with people in terms of the US visit with the FBI; IDENT 1, the police fingerprinting scheme; and the Hong Kong scheme where they can use ID to counter on-line fraud. All of these developments continually bring forward, first, that this is a concept of its time now and, secondly, that there are growing advantages. Different bits of the advantages appeal to different people, and that is what they will emphasise. That is why it is important we have our four main objectives. As I said, that should not exclude developmental work on using the card in other ways as time moves on.

Q1150 Chairman: One of our concerns as a committee is about the principal objective. Let us say that there is an agreement and the Government is clear about its four major objectives. I understand that different things could be added on in the future, but at the moment take those four things. What we find difficult to understand is how it is possible to decide on a technology which will be most suitable when you do not really know what it is that you want the technology to do. You have some objectives. You are going out to procurement but you do not know what it is you are going to procure in order to achieve your objective. We find that difficult to understand, or I as a simple person do.
Joan Ryan: I am clear about that. Obviously I have had many meetings discussing these issues with my officials and those who advise me on scientific issues in recent weeks, and only in recent weeks as I am newly in post, as you will understand. That is a very crucial part of understanding how this is going to happen. I think the committee is right to ask the question because these are large expenditures and we have to get this right. My understanding is that the reason procurement will happen in the way it does is that we do have clear objectives and so we know what outcomes we want. The technology that will be developed through procurement will be driven by the outcomes we require. We are not going to the market to buy something off the shelf. We are not saying to the market, "The technology must look like, feel like and act like this". We are saying that the technology must be able to deliver these outcomes for us. We will test that through the trialling. The private sector suppliers are the experts in developing the technology. We want to use their expertise and continually stretch them throughout the procurement process, but always testing and ensuring that we meet our objectives; i.e. the outcomes we require in order to establish the identity card programme.

Q1151 Chairman: You are now totally in the hands of the market to deliver an unknown product on which you may or may not meet the specifications which have been laid down by the Department?
Joan Ryan: I do not accept that we are totally in the hands of the market. You will know that in the first instance when we go out to procurement, the first phase will be when the market will produce for us a pilot or prototype where they will bear the risk and they will compete with each other. We will then have trialling of that small-scale production as to how we will enrol people and how the technology will work. At the end of that phase, we will select either a consortium or a private sector provider.
Chairman: You are confident that that is going to work.

Q1152 Dr Iddon: While we have been taking evidence, industry has been quite critical of the Home Office. I will give you a quotation from Microsoft, who, after all, are one of the biggest firms, in the field. They said: "After all these consultations we still do not seem to have had an impact on the level of understanding about what makes for a good identity system". On the back of that quotation from Microsoft, I would ask: is industry going to be entirely clear in the procurement process about what you are asking them to deliver?
Joan Ryan: You will know that we have, as I said, had a comprehensive market sounding exercise, and we have worked closely with industry and technical bodies using the industry routes such as Intellect. We

have also worked closely both with experts within the Home Office, through our Biometrics Experts Group, our Biometrics Advisory Group, across Government, through the Assurance Group and the Chief Scientific Officer and his panel. We have also looked very carefully at other schemes that are up and running. I cannot answer for any individual company's comment but I can say that we have worked closely with industry. We have taken a great deal of care to work closely with schemes that are already in operation. We are working with caution, I think it is true to say, to get these building blocks in place so that when we come to the procurement, we already have a large amount of evidence about the way in which biometrics are working. I think we are right to be cautious and to question. This is a big programme and a big expenditure. I am confident that the work we are doing with the market is in-depth work and that we will be able to move successfully through into procurement.

Q1153 Dr Iddon: It is not just Microsoft that are critical. Here is another criticism from another source. They say, and I quote, "You have people who are, frankly, scientists giving evidence to people who are, frankly, not". The implication there is that there are not enough scientists in the Home Office with which outside agencies and industry can engage at the same level and communicate properly.
Joan Ryan: Someone said to me on this position, "Don't you think it would be helpful if you were a scientist?" I said, "No, I do not. I think scientists are very helpful people and in fact I could say I am a scientist, a social scientist".

Q1154 Dr Iddon: I am not talking about you, Joan, but about the officers.
Joan Ryan: The point I was going to make is that I think we can demonstrate involvement at all levels of scientific and technological expertise both inside the Home Office and outside. It is also crucial that people who are not scientists are able to assess and understand this information and make a judgment about how confident we can feel in all the work that is being done. When we are running this out to the public, there is a huge issue of trust. We have a responsibility I believe, as Government and as Members of Parliament, to ensure that public trust and confidence in a project such as this is developed and maintained for all the right reasons. I think both scientists and non-scientists need to be able to understand it.

Q1155 Dr Iddon: What we are picking up, and it is not just in this inquiry but in other inquiries that this committee has undertaken, is that there used to be a scientific structure in the Home Office that seems to have been destroyed during the last couple of decades maybe and that the Home Office, when it comes to major procurement programmes like this, gets itself into difficulty because there is not enough technological understanding within the Home Office to be able to communicate with an industry that is going to deliver. Would you think that is a fair criticism or do you think the Home Office is well set with scientists and technologists able to handle this project?
Joan Ryan: I know that criticism has been made and there has been previous criticism of lack of a scientific culture in the Home Office. I also think that if we look towards the Home Office's Science and Innovation Strategy of 2005–06, which summarises the science in the Home Office and a series of reforms to invent science within the department, we can see that some of those concerns are perhaps not justified.

Q1156 Adam Afriyie: There are three main types of risk. We have a risk of time; it might take too long to deliver. We have a risk of money; it may cost too much to deliver. We have a risk of functionality; it may not deliver at all or it may not work. Which of those risks would you consider the easiest to mitigate—time, money or functionality—within each area?
Joan Ryan: All risks have to be mitigated. From what I have said previously to the Chairman about ultimately the issue of trust and confidence, the fact is that this is a large project involving large sums of money and all of those risks must be mitigated. If the honourable gentleman would like me to say a bit on each of those, I think we are working very hard to make sure that that de-risking does occur.

Q1157 Adam Afriyie: Perhaps you could say a few words on the type of risk in terms of time. You have a very tight time schedule here. I have 15 to 20 years' experience of IT projects. It seems almost inconceivable that you could trial new technology, develop it and have it deployed within the timescale set. Perhaps you could talk about how you are mitigating the risk of time so that all this does not take too long.
Joan Ryan: As I said, the timetable is not one that says to us, "Here is a ready-to-serve date. You must be rolling out ID cards at this point". We have aspirations built on some of the building blocks that we are putting in place, but the detail of the timetable will only become absolutely clear though procurement. That is as it should be because we would not be de-risking if we said to the committee, "We can absolutely guarantee to you that you will see the first ID card at such and such a date". If we did that, you would rightly say to me, "So are you going to learn no lessons through the procurement process? Are you going to learn no lessons through the trialling?" Obviously we have to work through the procurement process and the exact timetable will fall into place. I am sure we will have much more discussion about that as the process takes place.

Q1158 Bob Spink: Is the Minister now withdrawing the implementation timetable that had previously been announced for ID cards?
Joan Ryan: We do not have an implementation programme for me to withdraw, so I am not withdrawing anything. We do not have an implementation timetable.

Q1159 Chairman: We have been given evidence on that.
Joan Ryan: What we have been told is that there is a desire, and a strong desire, to see ID cards towards the end of 2008–09 being issued.

Q1160 Mr Newmark: Is that an aspiration or is that real timing?
Joan Ryan: That is a strong desire that we are working towards. As for the building blocks I have spoken about, I was watching ID cards being issued yesterday at Lunar House in Croydon. The ARC card for asylum seekers is, in effect, an ID card. You will know that from August every passport issued will be a biometric passport. All these building blocks are being put in place. We dealt with the secondary legislation on UK visas last week. By end 2007/early 2008, all UK visas will be biometric. That is a timetable and we are moving towards it, but that is not to say that I can give you a guarantee that the procurement process will have happened in a particular way.

Q1161 Chairman: To be fair, Joan, your predecessor did not give us a specific date either. We will not follow up on that. Risk is something on which we have not had a clear answer from you. Your predecessor appeared to be content to allow us to view the risk register. Why have you said no?
Joan Ryan: I hope I explained in my letter that there are potential confidentiality issues around parts of the risk register and obviously, at the point we go into procurement, this is crucial. Therefore, I took the decision that this could pose a difficulty.

Q1162 Chairman: What changed between your predecessor and you? Why am I not trusted to look at parts of the register?
Joan Ryan: Also, much of the register is outside the scope of this investigation. It is not a question of trust between myself and you, Chairman. I have said that I would be very happy, if you want to make a specific request, to do all that I can to meet that request and enable you to see those parts of the risk register within your specific request as it relates to the scope of this investigation and the work of the committee.

Q1163 Chairman: This inquiry is actually dealing with scientific evidence and risk. Particularly for those bits of the register that relate to science and technology underpinning the scheme, it would be very useful if in fact as a committee I can report back that we have actually seen the register and seen those elements of it and can say that that is happening.
Joan Ryan: I appreciate the point you are making and I would say that the offer I have made was very genuine. If you come back with specifics, then I will do all I can to accommodate that request. I understand that your desire is genuine and obviously the findings and the outcomes of the committee are helpful to us.

Q1164 Chairman: Of course they are and so I will be able to look at those elements of the register which refer specifically to the science and technology underpinning the scheme on a confidential basis?
Joan Ryan: I would ask the honourable gentleman, the Chairman, to respond to the offer made in my letter.

Q1165 Chairman: Why can you not just say yes?
Joan Ryan: I would like you to write to me with a specific request. It is important, with my responsibilities as an Under-Secretary of State, to consider carefully, particularly from a select committee, the requests that are made to me. I would like to give that consideration to your specific request. I can assure you that I will do that in good faith.

Q1166 Chairman: I find that very disappointing, if I might say so. One of the purposes of a select committee, particularly on an inquiry like this, is in fact to be able to have a trust between a minister and the committee. The idea that we cannot see and I cannot see elements of the register without going through a long process with you I think is disappointing, but there is no point in moving that on.
Joan Ryan: I am not saying you cannot, and I do hope that you will not be disappointed and that that trust will exist and does exist between us.

Q1167 Mr Newmark: Given that the Home Office has said that trials will provide vital new information, why is there at least a perception that this has been left so late? Is this not just increasing the risk of problems at a later stage?
Joan Ryan: That presupposes that no trialling has occurred, and I would not say that that was the case. First of all, there was some very important case work done early on in 2004 on the biometrics and technology options. There has been trialling since then. I would point to IDENT 1, which I think all are agreed has been a very successful procurement and build operation, and also obviously the IAFS immigration and asylum fingerprint system. The fact is that these are new, up and coming and existing programmes as IAFS is going to move into IAFS Plus to accommodate the UK visas and biometric resident's permit. They give us a huge amount of information and they are in effect trialling. However, that can only happen within the procurement phase because we want to trial what is being developed. We are able to do that in that first phase at the private sector's risk, which I think is a very good option for Government in procurement. Following that first phase, we will then, once we have our private sector partner and as the technology and the register are built, trial. For a system that will run for some 60 million entrants, we think somewhere around the first 2 million people registered into it will in fact mean very large-scale trialling. That is another reason why we are taking it a step at a time.

Q1168 Mr Newmark: According to the evidence we received on 8 May, there is not going to be that sort of trialling of specific technical issues.
Joan Ryan: We have used evidence from the US National Institute of Science and Technology that does world class biometrics testing.

Q1169 Mr Newmark: Let us move on. One of my concerns is about what happens if the technology actually does not meet up with the expectations in these live enrolment trials. Just to give you an example, and I am sure you have heard this two or three times at least, in women in terms of iris recognition there are changes at various times of the month.
Joan Ryan: No, there are not. The retina might change but the iris does not. I think we have clarified that.
Chairman: We have sorted that out.

Q1170 Mr Newmark: That was one of the things they were not confident about when we went to the States.
Joan Ryan: Brian raised it with me in Home Office orals. I would understand any concern like that. I am very pleased it was raised with me.

Q1171 Mr Newmark: I will come back to a more generic statement. What happens if the technology does not meet expectations during live enrolment trials?
Joan Ryan: You can see from what I have been able to say when you read the answer about irises that we are alive to these issues and these risks, and we are alive to them because of the work that we are doing looking at the deployment of existing technology and working with using evidence from bodies like NIST. I think that is a very important part of our trialling. Clearly, as I have said, we would build on that.

Q1172 Mr Newmark: By definition, you would not be trialling if you had total confidence in the technology.
Joan Ryan: I think it is best and good practice to trial and we would be trialling. We are confident that we will achieve procurement to deliver a technology that will deliver the programme, but I think your committee would rightly ask me what I thought I was doing if I was not insisting that there was trialling through the process. If I did not do that, you might be worried.

Q1173 Mr Newmark: Adam has been in high tech for 15 years and I have been in business for 20 years. Things never run smoothly and that is why I am curious. Have you any contingency plans in case there are problems during procurement?
Joan Ryan: As we are not tied to this exact timetable, that of itself is a contingency because if there are issues, then there is time to resolve issues. That of itself is a contingency. I think the real contingency is the fact that we are building gradually and it is incremental. That is because of the lessons we have learnt. I would say something else, and perhaps it comes back to the three risks that Adam mentioned, and add a fourth. If we look at what happened perhaps with the passport service, which is now an excellent service and one of our great successes and deserves to receive an accolade for that, as you all know, it had a difficult period, shall we say. That was not to do with the technology; that was to do with people issues—staff, training and enrolment. That is the fourth risk I would identify and it is another area we will be doing a great deal of work on. We are doing some of that work now through trialling, i.e. rolling out the biometrics passport and seeking to go to authentication by interview because it is not just about biometrics, you understand, establishing identity and issuing a card; it is also about a biographical footprint. That work is already going on as well.

Q1174 Dr Harris: To what extent is the scheme governed by politically imposed deadlines? Are you alive to the fact that there is a tension between the need to deal with pesky Opposition politicians who say, "No, this will be delivered" and scientific advice saying, "Wait a minute. There needs to be scope for wriggle room if problems emerge"? How do you balance that?
Joan Ryan: I hope what I have already said about the timetable you will find reassuring. I do not feel I am running this according to some political deadline. We have the legislation. We are moving to procurement. We are seeking to deliver, but I am not pressured by any external deadline outside that programme.
Chairman: That is good to hear.

Q1175 Dr Harris: If scientific advice said that the planned timescale, even if it is informal, is not reasonable because of difficulties, then that would count a lot. Do you fear that there is a culture that says that because this has become so political, it has to be delivered and the scientists will just have to get on with it?
Joan Ryan: I would like to go back to an earlier answer when I said there is another issue and that is about our responsibility to the public and the issue of trust. I do not think anything can be more important than getting it right. That would be my answer. I hope we can do that in a timely fashion, meeting a reasonable timescale, but nothing is more important than getting it right. If scientific evidence comes forward that tells us there is an issue, it will depend on the evidence. We will have to have that evidence assessed. I have no doubt we will be discussing it here. It would depend on what the issue is. I cannot comment on a hypothetical problem. I am not anticipating something major that would completely delay or derail the programme. I would like to reassure the committee that nothing is more important than getting this right.

Q1176 Margaret Moran: We have been told by the Government that facial recognition will be effective in protection and prevention of fraud as a central plank of what we are talking about here. Yet, we have received evidence from Professor Angela Sasse

to say that 90% of benefit fraud is committed by people who do not lie about their identity. What specific evidence do you have on the extent to which fraud is based on lies about identity? Could you also tell us how the ID card project will guard against this?

Joan Ryan: I think it is the case that the majority of benefit fraud is not perpetrated at present by people who are lying about their identity, as far as I am aware. Given your question, I will ensure that I look at specific evidence. That is my understanding. We would say that where there is a level of benefit fraud which relates to identity, then clearly it is important that that is tackled. Clearly, in that case identity cards will help. As I mentioned, there is the issuing system in the Hong Kong system. These technologies are developing. The way in which people access services and markets is changing. Much of it is internet-driven. We know that the ways in which people can commit fraud, in terms of use of identity and credit cards and all kinds of issues and stealing other people's identities, is on the increase. We know that these measures will help. I cannot put figures on that here and now for Margaret but I will of course look more carefully at that. I think what you say about benefit fraud is in fact correct.

Q1177 Margaret Moran: You referred to yourself earlier as a social scientist. We have heard from the Home Office that social science is being used to validate assumptions and that where that research rejects a current assumption, a change is made. Could you give us a specific example of where that has been the case, where social science has influenced a change of direction in a project?

Joan Ryan: I can say that we have undertaken nine separate pieces of social science research, and so we do think this is very important. One of the pieces of research is looking into people with special needs issues. We have undertaken 16 focus group discussions. Certainly, from all that we have learnt from that, it is not so much that we make an assumption and then change it; it is that we are learning from that kind of work and from the other social science I have mentioned done with the public. We are learning from them what the issues for them will be. I mentioned special needs in particular because you will know from the UK Passport Service that we have done trialling and we have found that elderly, people with various disabilities and some minority ethnic groups had more difficulty enrolling than others. That was not necessarily to do with technology.

Q1178 Chairman: Have you changed the system as a result of this?

Joan Ryan: It is informing the way in which we are enrolling people and the way in which we are enrolling them for a biometric passport. That will inform how we are going to enrol obviously for an ID card because a passport is the designated document. I am struggling to think of specific changes that we have made. We know that there are issues for people about how easy it is, given various disabilities, for them to deliver their fingerprints, whereas facial recognition is much easier.

Q1179 Chairman: Would it be possible for you to look at that and perhaps let us have in writing some ideas on the way you conduct the social science research and the way it has affected the programme is moved on?

Joan Ryan: I would be delighted to do that. As I say, there has been a lot of work done there. I would appreciate giving the committee more detail on that.

Q1180 Margaret Moran: The Gateway Review has been completed but that focuses on process. Could you tell us whether you are prepared to undertake a gateway review on the practical and technical feasibility of the project and make that available?

Joan Ryan: I would have to ask to write to the committee on that. I would need to understand the gateway review process and how it has been applied so far to this process and also to biometric residents' permits. I do not feel I can answer that at the moment.

Chairman: That will be acceptable.

Q1181 Dr Harris: You said you are not aware specifically and you will let us know of any specific changes that have been made following social science research. We are told in your evidence, and I quote, "the mechanism for incorporating the results of social science work into the programme is predominantly a robust change control process". Do you know what that means because I do not, I am afraid.

Joan Ryan: I think it means exactly what Margaret was saying. We undertake this research and from it we are able to acquire information about how best to do things like enrol people and deal with people's issues. One of the things we were interested in finding out from people was whether they felt that giving fingerprints meant that in some way that you are a criminal. There is a lot said about people's perceptions being that if you are asked to give your fingerprints, there is some notion of criminality and people would be very resistant to do this. We discovered through the research that that is not the case at all. People's attitude was pretty much: if you have nothing to hide, why would you be worried? We also discovered, through things like the biometrics road show, that people quite like testing out the technology and that, far from it being a barrier, the only times when it hit the barrier might be when there are physical reasons why it is difficult for people to use the technology. There are other issues as well, cultural issues. We have seen these through the roll-out of the passport as well and the new photograph in order to get the facial biometric; for instance, the wearing of head wear for certain groups is an important issue. Social science research has helped inform us about to how to deal with and approach those issues. It is not so much making a complete change from one idea to another but it is informing us about how to approach and handle these issues.

Q1182 Dr Harris: Can I ask you about costs? To what extent would costs be a driver in choosing the technologies, or indeed the functionality? How do you balance costs?
Joan Ryan: I suppose we would want what is called best value in that the cheapest will not necessarily be our choice because it might not be able to deliver what we need to see delivered. Our business case has been seen by KPMG. It has been through the Office of Government Commerce gateway. It has had approval at many levels. We are confident that we have the funding and the costings, that they are robust, and we have built in contingency, optimism and bias. We feel we are going to be in a strong position in relation to cost and procurement, but clearly the priority is that we are confident we are (a) getting value for money but (b) that it will deliver.

Q1183 Dr Turner: Could either of you tell us something about the "joined-upness" of working between government departments on the ID scheme, both on the technology development and making sure that other departments can use it without any operational difficulties. Obviously the Department of Health is going to have an interest in this; DWP is going to have a considerable interest. What can you tell us about that aspect?
Joan Ryan: We have undertaken a great deal of work on what we call stakeholder engagement, which is what I think you are referring to in terms of the development of the identity card. We have also undertaken work with our delivery partners and then with other groups as well, such as industry groups and a technical group. Across government, the ID card programme managers are key stakeholders who may expect to realise benefits from the introduction of the scheme. We have account managers and they have been in place since 2004. They each have a key contact person at strategy board level. We draw in from that DWP, Department of Health, CRB, the police, and the Department for Communities and Local Government.

Q1184 Chairman: Are these contacts at ministerial level?
Joan Ryan: No, these are at civil servant level. Through that work, obviously we are attempting to get this cross-departmental recognition of benefits, the buy-in and working together. We also do that through working on our building blocks.

Q1185 Dr Turner: You will have taken steps to ensure that the technology is compatible across the whole piece?
Joan Ryan: Yes, it is absolutely crucial that interoperability exists. We have a number of ways in which that is being approached. We also ensure that with all other schemes we have the technical specification whereby everybody is going to be able to speak to each other.

Q1186 Dr Turner: One of our witnesses suggested that there has not always been the coherence that there might have been. Specifically they referred to the e-Borders programme where it is suggested that there has been a lack of sharing of evidence, a duplication of effort and a general overlap. There is a specific claim that there has been little coherence between the programmes, particularly in the early stages. What comment do you have to make on that?
Joan Ryan: In terms of interoperability, we have common technical standards as a start point. We have the e-Government Unit and the Government's Interoperability Framework. We work within that. Across departments, we have our stakeholder groups and our expert assurance groups to make sure that is all working together. You brought up the example of e-Borders. The e-Borders Programme has its own timetable. Although we would look to learn from particularly Project Iris for instance and issues around iris scanning, e-Borders and iris scanning do not actually have a card that relates to the database in that way. It is not perhaps as close a building block to the ID card scheme as some of the other building blocks I have mentioned. It would not be correct to say that there is no interaction between our e-Borders development team and the ID card scheme because there is and it is very important. I am not sure the relationship between what is being developed in both these things is as close as the relationship with UK Visas and biometric residents' permits.

Q1187 Bob Spink: Given the technological implementation uncertainties and the massive IT infrastructure requirement, procurement will, I guess from your answers, be a developmental process. Will it therefore be on a fixed-price basis, or are you returning to the old cost-plus contract basis for this procurement? Both of them have their problems.
Joan Ryan: I am loath to delve into talking about the cost issue at the point where we are about to go to procurement because I do not think that would be most sensible. At the point where we talk about that, we would want to discuss it.

Q1188 Bob Spink: I think that we as a committee and Parliament generally have a duty to hold the Government to account. If the Government is going to return to a cost-plus rather than a fixed-price contracting basis, then I think that is something of public concern.
Joan Ryan: We have given quite detailed information as far as we are able, without breaking commercial confidentiality or going outside the scope of the committee, on the business case. That is in the public domain. You will also know that we have undertaken every six months, subject to commercial confidentiality, to submit a report to the House of Commons, and that was agreed at the Lords' Amendment Stage.

Q1189 Chairman: It was and we are content with that. Joan, thank you very much indeed for answering all these questions. We will have further questions later in the session. Can I briefly ask you this? Last week we had Paul Wiles in front of us, the department's Chief Scientific Adviser. We

specifically asked him whether he had responsibility for ICT in the department and he said "no". Neither he nor in any evidence we have received from the Home Office have said who is responsible for ICT. Do you know who it is?
Joan Ryan: Could I ask to write to the committee on that point to confirm who I think it is?

Q1190 Chairman: That is interesting because it is actually Vincent Geake. What we would like to know is why in fact he has not been mentioned in any evidence at all and why you as the Minister did not know and neither did the Chief Scientific Adviser. Perhaps you would write to us on that issue because IT seems to be incredibly important to this project.
Joan Ryan: Obviously he is the Chief Information Officer. I was just a bit thrown when you said "technology". I do in fact know that that is his job. Also, he is newly appointed and so I was struggling to find his name, but I do in fact know it is him.

Q1191 Chairman: It was not a trick question but just that it is an important issue. Thank you very much indeed, Joan. We will return to you. We move on to Vernon Coaker and the issue of drug classification. Could I launch in straight away, Vernon, and say that the Chief Executive of the Medical Research Council described the current classification system, and I quote: "It is antiquated and reflects the prejudice and misconceptions of an era in which drugs were placed in arbitrary categories with notable, often illogical, consequences". Do you agree?
Mr Coaker: No, I do not agree with that.

Q1192 Chairman: Why not?
Mr Coaker: I think it is a fairly extreme view and I am sure it was meant to actually put a point of view. I think the classification system has generally served us well. There is a basis for the classification of the drugs. I think it is a system that is understandable to people and has credibility with the public.

Q1193 Chairman: You would defend it, as the Minister responsible?
Mr Coaker: I would defend it. That is not to say it is perfect.

Q1194 Adam Afriyie: Could I go back one step? What do you consider to be the aim of the UK drugs policy and the classification system in particular? Obviously we want to see drug use stopped. Is the policy to stop the users, is it to stop dealers, or is it to stop the suppliers? What is the aim of the policy of the classification system?
Mr Coaker: That is a very good question. It is not either/or. Sometimes, in these debates about drugs strategy, we get into an either/or situation. As an overall strategy, it is about tackling drugs, dealing with the street, trying to tackle that in terms of crime on the street and doing something about some of the problems that people see on their street. It is about getting more people into treatment, trying to do something about those people who are misusing drugs, and trying to support them. If you look at the numbers going into treatment, there is a record number of people going into treatment at the present time. It is about breaking that cycle. Alongside that, it is also about education and changing attitudes. I think the classification system helps in the sense that it identifies those drugs which are potentially harmful.

Q1195 Adam Afriyie: I am somewhat surprised that you argue that the classification system has been helpful when drug use has increased enormously since the introduction of the classification system. What does that say about the classification system when in other countries like Sweden drug use has virtually gone?
Mr Coaker: We have a situation where we have a drugs strategy that is tackling drug use out there; it is tackling the prevalence of drugs on the street and drug use. If we look at some of the statistics, in terms of the drugs strategy, we are seeing a degree of success with 16–24 year-olds. The 2004–05 British Crime Survey compared the present situation to 1998 and for 16–24 year-olds the proportion that reported that they had ever taken any drugs had fallen by 15%.

Q1196 Adam Afriyie: If we go back to when the classification system was first introduced, then I think the picture would be very different. It is easy to point at a graph, take a couple of dates and make a case. If you look at the overall picture since the introduction of the classification system, the evidence is completely the other way round, is it not?
Mr Coaker: If you go back to '71, we were in a different type of society. We are dealing with society and the community as it is now. I think in that sense we have a situation where there is an overarching drugs strategy, which is not just based on the classification system but on education; it is about changing attitudes and it is also about enforcement of the law. It goes back to what I said earlier. It is not one situation or the other; it is a package of measures trying to deal with the problem we have.

Q1197 Adam Afriyie: What precise or specific evidence is there that putting a drug in a higher class actually has a deterrent effect? From what I can see, sometimes it even seems to have the reverse effect.
Mr Coaker: I think that people out there—if we talk about the population in general, the public at large—if we have classified a drug as a Class A drug, realise that it is a serious drug; they realise that it is a drug that is harmful. It is a drug that has a particularly—

Q1198 Chairman: Where is the evidence? I am not doubting that you believe that, but where is the evidence to demonstrate your response to Adam's question?
Mr Coaker: The evidence is in the survey that we have taken recently where we have looked at drug use, and the statistics that I have just given out, where we have seen a reduction in the use of drugs.

Chairman: The point of Adam's question, if I get him right . . . . I am sorry, Adam, perhaps you should ask the question.

Q1199 Adam Afriyie: The point of the question is this. What specific evidence is there that when you move a drug to a higher class there is a deterrent effect on its use? Where is the evidence for that?
Mr Coaker: We take the advice of the ACMD; we take the advice of the police. The ACMD has scientific representatives on it. They are people who are professors of pharmacology, and so on. They advise us on that, and they advise us on the class of drug, where a drug should be classed, and we take evidence from them. Then that gives us the opportunity, as I say, to reflect on the impact that has on the public.

Q1200 Dr Harris: However, Professor David Nutt, who is the Chair of the ACMD Technical Committee, says, "I think the evidence base for classification producing a deterrent is not strong". So, on the basis of what you have just said, will you now take that away and change your answer? If you are referring to him, he disagrees with you by 180°.
Mr Coaker: Professor Nutt, as you know, is a member of the ACMD. We have a matrix which we use. That matrix is part of the way we determine which drug should be in which category. Of course, we always look at the evidence that people give us; we always look at the opinions that they give to us; but what we have there is Professor Nutt being part of the ACMD and we take his advice.

Q1201 Chairman: It is disturbing for the Committee—and this is about evidence and policy, Vernon, not about whether the Government's policy is right or wrong. What we are saying is this. Is there any occasion when the Home Office has commissioned research to show that when you put a drug into a higher classification it actually has a deterrent effect—or the opposite?
Mr Coaker: We have a scientific basis for determining harm. The ACMD refer to that when they classify drugs. When we come on to methylamphetamine, they risk-assessed that against the matrix, and that is when they have come forward with the proposals they have with respect to that drug.
Chairman: We will return to that specific drug.

Q1202 Adam Afriyie: I have just one last question around evidence and research. Have you commissioned any research to look at the classification of a drug and the level of crime associated with it? It does seem from studies in America and elsewhere in the world—I am not sure about the UK because I have not seen the research here—that if a drug is in a higher class, it therefore has a higher perceived street value; dealers get involved; there is a higher economic incentive for crime. Have you commissioned any research into that area?
Mr Coaker: The Department of Health carry out a lot of research and we work closely with them. They commission a lot of research into different aspects of drugs. I have here a number of reports, both by the Home Office and by the ACMD, which research into various aspects of drug and drug abuse.

Q1203 Adam Afriyie: Do they look at the class of a drug and the crime associated with that and the correlation between them?
Mr Coaker: There is an obvious example with respect to that recently. As Phil was saying, we will come back to the methylamphetamine. Cannabis is an example of a drug that they looked at and did some research into. Ketamine is another one that recently the Technical Committee looked at and, obviously, date rape. So there are a number of research projects which are going on at the present time, looking into various drugs—both recently and now.

Q1204 Chairman: Coming back to the ABC classification, in January the then Home Secretary announced that a consultation paper on the ABC classification system would be published within a few weeks. It has still not been published. Why?
Mr Coaker: I am sorry, could you repeat the question?

Q1205 Chairman: In January the then Home Secretary Charles Clarke announced that a consultation paper on the ABC classification system would be published within a few weeks. There was obviously a concern about it at that time. Why has it not happened?
Mr Coaker: Two things. First of all, the Home Secretary—in post for four weeks—has not yet taken a decision on how to proceed with the review of the classification system. With respect to the consultation document which is in draft form in the department, the view is that we will need to wait until such time as we decide how to proceed with respect to the review of the classification system and also, similarly, wait for the report of this Committee—which we want to take into account in determining the best way forward.

Q1206 Chairman: That is a very honest reply, if I may say so.
Mr Coaker: I am trying to be helpful.

Q1207 Chairman: Of course you are. Do you think, as the minister responsible now, the classification system should be directly related to the penalties for possession and trafficking? Do you think there should be that direct relationship between classification and penalties?
Mr Coaker: I think that the classification system is based on harm, and there is a relationship therefore between harm and the penalties that should be apportioned to them, according to that classification. Yes, I do. Class A drugs, for example, are regarded as the most dangerous drugs and

therefore in that sense the penalties associated with possession, supply, et cetera, correlate to that degree of harm.

Q1208 Chairman: So the greater the degree of harm of the drug should then attract the highest penalty?
Mr Coaker: That is a matter for the courts in the end, as to what they actually think; but certainly that is the way the legal system is based—on the potential harm.

Q1209 Chairman: Do you support that? Do you support that classification equals penalty?
Mr Coaker: Classification equals the degree of penalty which is available to the courts.
Bob Spink: Could I get clarification? Will methylamphetamine be reclassified as a Class A drug?
Chairman: You can answer that when we get on to that section.

Q1210 Mr Newmark: Is there a need for a more scientifically based scale of harm to be developed to facilitate education and debate, with an emphasis on a scientifically based scale of harm?
Mr Coaker: I referred earlier to the way the ACMD—which is the statutory body that we have to consult—have a harm index, which includes taking into account some of the scientific evidence that it gets. It also takes into account social harms, and so on. So there is a degree of assessment which is made, according to the matrix that they use.

Q1211 Mr Newmark: That is a form of matrix. I am talking specifically on the science of harm itself.
Mr Coaker: But they will receive reports; they will receive evidence; they will look at various things that are happening, and get people coming to them to talk to them. So scientists will come to them and talk to them about their scientific beliefs, their research. People will come to them with reports about what they think about particular things. The ACMD can take that into account when they are determining the way forward. The science plays an important part in the determination of the ACMD's conclusions.

Q1212 Mr Newmark: I am not sure if you have answered my question but, given that you put great stock in the ACMD, how do you respond to findings by experts, including the chairman of the ACMD Technical Committee, that tobacco and alcohol are more harmful than LSD and Ecstasy, both of which are classified as Class A drugs?
Mr Coaker: There is an important point to make about the ACMD. We put great store in what they say. We listen carefully to the comments that they make. However, it is not a cosy relationship; it is a challenging relationship. They will challenge us in a whole variety of areas. I think that is as it should be. It is an independent body. It is a body whose opinions we respect, and we try to work closely with them.

Q1213 Mr Newmark: Do you disagree then that tobacco and alcohol are not as harmful as those two particular drugs?
Mr Coaker: Alcohol and tobacco are legal drugs, and they operate within the framework of our society.

Q1214 Mr Newmark: But they are very harmful, are they not?
Mr Coaker: They are harmful in many respects, if abused—or alcohol, if abused. But they are socially acceptable drugs; they are drugs that most of us, particularly with respect to alcohol, will use sensibly. If we are looking at the real issues of society, alcohol and tobacco clearly are issues which, if abused—alcohol if abused, and smoking, as we know, is harmful—we are trying to combat, in terms of the abuse of alcohol and, in terms of smoking, trying to reduce that as well. However, they are legal drugs and we have to look at them within the context of the society in which we all live.

Q1215 Mr Newmark: How will that sort of thinking that is coming out of these experts influence future policy decisions on crime, with respect to drugs, crime and public health?
Mr Coaker: In terms of where we have particular representations made about drugs which are harmful, where they are talking to us about different things, then—as I was saying earlier in reply to Adam—that is the other aspect of drug policy, which has to be an enforcement policy. There has to be a policy which is out there, trying to tackle the supply and those people who deal in it on the streets. We have taken a number of measures in order to try to deal with that as well. For example, if you look at the recently established Serious and Organised Crime Agency, that has, as a very real focus and as one of its top priorities, the tackling of the supply of drugs.

Q1216 Mr Newmark: Why is it that in the UK spending on addiction research is so much lower per head than, for example, in the US? Is this a reflection of it being a lower priority over here versus over in the States?
Mr Coaker: We massively increased the spending on drugs, on trying to tackle the harm which drugs are causing in our communities. The drug treatment programmes, the establishment of the various projects that we have, have seen a massive increase in spending.

Q1217 Mr Newmark: And when it comes to addiction research?
Mr Coaker: With respect to addiction, there are priorities that people have. The health service and all the other bodies have seen big increases in spending. Do we want to see more spending on that sort of research? I think that is a legitimate question to ask and something we should look at.

Q1218 Mr Newmark: So would you like to see more money spent on it?
Mr Coaker: I think that it is something we should look at, yes.

Q1219 Mr Newmark: Do you feel that the lack of evidence in this area is actually an impediment to evidence-based policymaking itself?
Mr Coaker: You have taken evidence from the ACMD, but I think that they would say that their advice to us is evidence based. They take evidence from a variety of sources and, in taking that evidence, they make recommendations to us. I think they would say that the various reports that come to us, the various recommendations that they make, are based on evidence which they have taken and considered.

Q1220 Dr Harris: I do not think they do say that. Let us be very clear, because you have said three times now that you take advice from the ACMD; that the ACMD appear to take evidence; and that you are happy and they are happy that there is evidence. I quote Professor Nutt who chaired the ACMD Technical Committee, who argued to us that a more scientifically based scale of harm would be of value in the situation. He said, ". . . in education the message has to be evidence based. If it is not evidence based, the people you are talking to say it is rubbish". He co-authored a report that said that, with respect to the correlation between the class of a drug in the current ABC system and its harm score, calculated using their—I would say scientific—approach, was so low that it was "not statistically significant". So your main source of advice says that there is not enough evidence out there and the ABC classification in relation to harm has a non-statistically significant correlation. You should be furious about this: that your whole policy is based on an evidence vacuum.
Mr Coaker: We do not believe that it is based on an evidence vacuum. There is always a need to improve; there is always a need to look at the evidence that you take. However, as I say, the Nutt matrix forms part of the harm index matrix that the ACMD uses itself in order to determine the recommendations they make to us. They have a number of headings that they use. There are priorities within that. They score that according to the various priorities. There are nine priorities, I believe, and they score that. Then that determines the recommendations they make to us. So there is a matrix; there is a harm index which they use. That itself is influenced by Professor Nutt's criteria.

Q1221 Chairman: Why is he so critical, though?
Mr Coaker: That is something he has every right to say. We will always look at people who have criticisms to make; suggestions about improvements, and so on. The point I am making, however, is that the ACMD—which is a statutory consultee for the Government—does work according to a harm index which it uses to score drugs which it believes to be harmful. We will come back to a drug where it has actually used that in order to determine harm. It is fair comment and we will need to look at the comments Professor Nutt has made. That may be his individual view but, as I say, on the ACMD we have that harm index which is used by them.

Q1222 Dr Harris: Professor Nutt's quote that I gave was from a paper where he was calling for the scale to be a rational scale of harm. You say there is evidence. Are you aware that the amount we spend per head of population on addiction research is a hundredth what the Americans spend, and that the budget is somewhere between a hundredth and a thousandth? That is not a judgment call as to whether we are not spending enough versus other priorities. It is just 1% per head of the population of what the Americans spend.

Q1223 Mr Coaker: On . . .?

Q1224 Dr Harris: On research into addiction—which would include the evidence base around this. It is a real problem.
Mr Coaker: As I said to what Brooks was saying, the money that has been made available to drug treatment programmes and this whole area of work has increased significantly. There is always the question of where you spend that money. It may be addiction that should have more spent on it, alongside some of the other priorities that you have. So there is always a scale of priorities. One of the things we can do as a result of the report that the Committee will no doubt make about it is to have a look at that, to see whether it is appropriate for us to look at the amount of money that has been spent on it.

Q1225 Dr Harris: To what extent do headlines in the newspapers influence, as a politician, your policy in this area? Do you use the newspapers as a proxy for public opinion?
Mr Coaker: No, certainly not. We try very hard to have a drugs policy, which we drive according to what we think is in the best interests of the population and the best interests of the communities that we all represent. Going back to what I thought was Adam's very important point at the beginning, about what is the purpose of the drugs strategy that we have, as I say, it is about enforcement; it is about education; and it is about drug treatment. Obviously, within that there will be disagreements and debate about the best way of delivering all of those objectives. We are not driven by headlines; we are driven by what is best for the people that we seek to do our best for.

Q1226 Adam Afriyie: If there were a town, a city, or a country elsewhere—outside Britain, obviously—that had been almost totally successful in reducing the use of drugs and in getting rid of the harmful effects of acquisitive crime around drugs, would you be willing to look at that example, even if it meant that you had to re-look at the classification system?
Mr Coaker: I think that it would be very arrogant of anybody to say they would never look at what anybody else is doing, or try to learn. Indeed, part of what the Select Committee itself is about is to make recommendations to government about how to improve policy. Obviously, you have to look at that and consider it. Whether you then say, "This is applicable to our situation; this is applicable to our

communities; this is something that we will do", is a different matter; but certainly you should always look at what is going on, try to learn from other people, and see whether it is applicable.

Q1227 Chairman: Our concern, Vernon, is the way in which the Home Office goes about researching, getting proper evidence on which to make its policies. That is a genuine concern for us, which is why we are bringing this to you.
Mr Coaker: That is fine.

Q1228 Dr Harris: Do you think decisions on classification should—I think that you are saying this, whatever we think of the evidence base—be based on evidence of harm and therefore we classify on that basis, or should it be to send out signals to the public?
Mr Coaker: I think that what the classification does is categorise drugs according to harm. I also think that it does send out messages; it does send out signals to people, in a way which people understand. I think that most people, if you talk to them, would understand that Class A drugs are the most dangerous drugs. That is the advice we have received from ACMD, from the police, and so on. So I think that it is a balance of those things.

Q1229 Dr Harris: Andy Hayman, who chaired the ACPO Drugs Committee, told us in oral evidence, "I cannot envisage any user—a dependent user, that is—having any kind of thought as to whether it was a Class A, B or C drug they were consuming". I think the advice he would give, therefore, is that you cannot really send out messages to addicts with your classification system. I am saying that it has to be based on harm.
Mr Coaker: But is not part of any system with respect to drugs—as I think the Government would argue, and I would argue—not only trying to send messages out to people who misuse drugs but also about trying to send messages out to people out there in the community? So that when teachers are in schools, the parents are there, or the police are working, or whatever, there is a message there about which drugs are regarded by society as the most harmful. I would argue that it is about that as well.

Q1230 Dr Harris: If it is about that, then surely there should be evidence as to whether that is having any effect? Are you aware of any Home Office-commissioned evidence about the impact of the messages that you are trying to send out? Because if there is not any, then it is just rhetoric, is it not?
Mr Coaker: It is not just rhetoric, in terms of where we were before. The evidence base for us with respect to the last few years has been in the reduction of drug misuse. It has also been in the evidence that we receive from the ACMD, who advise us on these matters. We come back to this. If this is so unimportant in that sense—or not "unimportant"—if it is so unnecessary, why is it that people make such a big thing about the importance of reclassifying particular drugs? They do that because of the message that it sends out to people, and the belief they have that, by doing that, it sends an important message to people—which helps in controlling the prevalence of that drug.

Q1231 Margaret Moran: Coming on to the ACMD, we have had evidence from a variety of sources who raised concerns that this independent advisory committee is perhaps not functioning as well as it should. There was concern about the appropriateness of membership, about its expertise and transparency. Mary Brett, who is the UK representative on the board of Europe Against Drugs, asked the question, "Where are the biologists, the neurologists, toxicologists . . .? . . . there is not a single member of an anti-drugs charity". In other words, in her words, "[the] committee lacks any sort of balance". Where is the independent evaluation of the quality of the ACMD's advice, given those levels of concerns? Would you support the introduction of a regular independent review?
Mr Coaker: As you know, the Home Secretary appoints the people to the ACMD. Looking at the list, I would say that there is a fair cross-section of people from across society. Does it always mean that every single section and part of society is actually represented? There is always a case for continuing to look at that; for continuing to make sure that the balance is there. We value very highly the advice we get from the ACMD. We believe that it is independent advice. We believe that it challenges us—which is very important. I think that we need to continue always to look at how we improve—

Q1232 Margaret Moran: I was asking specifically about independent evaluation by the Government of the quality of advice that is being offered, and regular reviews of the quality of that advice.
Mr Coaker: We always reflect on the advice that we get from the ACMD. Whether there is a case for us to reflect on how we might improve that, what more we might do, is comment we need to listen to and to think about. However, the advice comes in to us from there and we often take further advice on the advice we have received from the ACMD. We often consult with other bodies about it as well.

Q1233 Chairman: Who do you consult?
Mr Coaker: We may go out and we may say, "This is the advice". We talk to other ministers. We listen to what other people have to say. These things can often be a case for us listening to what others have to say about the information that we get.

Q1234 Chairman: With respect, other ministers will not give you the sort of evidence that Margaret is asking for, in terms of that independent review. Who else would do it?
Mr Coaker: An independent review? Obviously, as ministers, we often go out to consult with people about—

Q1235 Chairman: Like who?
Mr Coaker: Not formally, but we informally talk to charities or others about the sorts of policy directions that we have, and listen to what they have to say. For example, only last night drugs charities were in the Home Office, being asked about their views and opinions about the drug policy. So there is a whole variety of ways in which things feed into the decisions that are actually made. There was a formal event at the Home Office yesterday. Lots of drugs charities were there, lots of stakeholders there, talking about—

Q1236 Chairman: So it is a purely ad hoc process. That is what you are saying?
Mr Coaker: But there is a process.

Q1237 Margaret Moran: We talked about the balance of expertise of membership. I referred to that and so did you. The question then is who is appointing this independent panel. Do you not think that the chairman of the committee plays an overly influential role in appointing the panel? Surely the Chief Scientific Adviser should have some role or oversight in this?
Mr Coaker: The Home Secretary, in the end, is the person who determines the membership of the committee. Looking at the membership we have, I think that there is a fair reflection of the various sections of society across the board who are members of the committee.

Q1238 Chairman: But it is dependent on the chairman. That is the point that Margaret is making.
Mr Coaker: Dependent on the chairman to advise him as to who should be on that, but the Home Secretary in the end makes the final decision.

Q1239 Margaret Moran: Where is the Chief Scientific Adviser in all of this?
Mr Coaker: Again, who the Home Secretary consults, who the Home Secretary listens to—he will get the recommendations and he will take advice accordingly.

Q1240 Margaret Moran: So there is a formal role for the Chief Scientific Adviser?
Mr Coaker: As I say, the Home Secretary will get the suggested people who should be on the committee or who should be members of it, and he will make the final decision.

Q1241 Chairman: I would really like to know your views on this. The previous Home Secretary and the Chair of ACMD seemed to disagree about the role of ACMD in considering social harm. Charles Clarke said, ". . . clinical, medical harm is the advisory council's predominant consideration". That was backed up by Andy Hayman who said, "What is directing which classification a drug goes into is the scientific and medical harm". However, Sir Michael, who is the chairman, contradicted this by telling us that social harms were given "equal weight" in the committee's deliberations. What is your view?
Mr Coaker: The committee's deliberations on it include social harm, and I think that is an important consideration.

Q1242 Chairman: Sir Michael says, "given equal weight"; the previous Home Secretary said no to that and Andy Hayman said no to that. What is your view?
Mr Coaker: My view on it is that the committee have a number of things that they consider alongside social harm. They consider physical harm, withdrawal, pleasure, and so on. So they take a number of things into account as well as social harm. I think that the balance the ACMD currently has is right.

Q1243 Chairman: So you agree with Sir Michael rather than the previous Home Secretary?
Mr Coaker: No, I agree with what was being said before—the previous Home Secretary—that it is the balance, where you have physical harm, pleasure, withdrawal, as well as social harm.

Q1244 Chairman: No, the previous Home Secretary said, ". . . clinical, medical harm is the advisory council's predominant consideration". You agree with that, and not Sir Michael Rawlins, who says that the whole issue of social harm should in fact be given equal weight.
Mr Coaker: Social harm should be included in the research harm index which they do, which it currently is. So I agree with what Sir Michael is saying: that it is not only social harm; it is physical harm; it is pleasure; it is all of those sorts of things. That is the matrix that the ACMD currently use to help prioritise what their decisions are.

Q1245 Chairman: You agree with both of them, but they take contrary positions. That is not tenable.
Mr Coaker: No, what I am saying is that the research matrix, the harm index that the ACMD currently use, is a tested thing. Social harm is a part of that. It has a number of priorities within it, and social harm is one of those; but, alongside that, physical harm, pleasure and withdrawal also have to be used. So Sir Michael is right in pointing out that those are the things that they use to consider their decisions.

Q1246 Chairman: In terms of the role of the Association of Chief Police Officers, we were somewhat confused by the response we had from Andy Hayman about the role of ACPO on the committee. Do you feel that ACMD should consider evidence from the police in its deliberations, or is it for ministers to integrate that advice from police with advice from ACMD? We were concerned that he did not see it as his role to initiate anything on ACMD, even though he is representing all the police forces in the UK. What is your view?
Mr Coaker: My view on it is that Andy Hayman and indeed Howard Roberts, another senior police officer who is on the ACMD, play a very important role on the ACMD. I think the role that they bring to it is the knowledge they have of policing and law

enforcement in this particular area. It is that professional expertise which they are bringing to the committee, and that sits alongside all the other sorts of people you have on that. My own view is that, as well as reflecting the view of the police, they bring an independent voice to it, which is about law enforcement and the practical implications of the policies that the ACMD are considering.

Q1247 Chairman: Vernon, here is the rub. The police forces do collect evidence about the effects of drugs on the streets and how it interfaces with crime. They have that evidence. If we were going for evidence-based policy—and you have agreed that the ABC classification should in fact have a link between the degree of harm and punishment—surely the police, through their representatives, should be initiating advice to ACMD rather than just being there to comment on what is going through the committee?
Mr Coaker: ACPO will—

Q1248 Chairman: He said no. He specifically said no, that was not their role. He was there to deliberate rather than to initiate. I just want to know whether you think that he should be initiating rather than deliberating.
Mr Coaker: If he is in the committee, he will be informing the committee of his view based on his experience and the experiences of the police forces throughout the country. That is part of why he is there. He is there as a voice of police experience, if you like, as is Howard Roberts.

Q1249 Chairman: That is not the point I am making. The point I am making is that, if we are looking at evidence-based policy here, the police have a vast amount of evidence to bring to the committee. That does not appear to be happening. Do you think that it should?
Mr Coaker: You would expect and hope that the police are bringing that knowledge and experience of dealing with these issues to the committee. In my view, that would be why they are there: to bring that experience, knowledge and understanding to the committee—both with Andy Hayman and with Howard Roberts. Clearly ACPO sometimes, outside of that, will come to us about other matters and other issues.

Q1250 Dr Iddon: Could you confirm to us this morning that the Government is considering reducing the amount of all drugs, including cannabis, which individuals will be allowed to carry and bring them at risk of being charged, instead of with possession of the drug, with possession with intent to supply a drug? That brings a maximum sentence of 14 years in jail, of course.
Mr Coaker: As you will know, as a result of the Drugs Act, at the present time we are considering what the thresholds should be, in terms of coming to a conclusion as to what it should be for presumption of supply. No decisions have been made at the present time; but we are looking at that, yes.

Q1251 Dr Iddon: Will Parliament get a chance, either on the floor of the House or in delegated committee, to debate any changes, or can the Home Secretary do this without consultation?
Mr Coaker: No, it is affirmative resolution, so it will have to come before the House with respect to determining these thresholds.

Q1252 Dr Iddon: Will there be wide consultation with outside agencies before any decisions are made?
Mr Coaker: We have already consulted with different people. There was a consultation exercise which started in January and ran till March. Those consultations are currently being considered and, just recently, we have had the ACMD letter come back to us which has given us their view. We will take their view into account, and we will take into account the other consultations which took place in the three-month consultation period, before coming to a decision as to what we should do.

Q1253 Dr Iddon: We have changed the classification of cannabis from B to C; we are now considering changing it back again, from C to B. We are considering changing the amounts that people can carry, related to the charges that might be imposed upon them, and the previous Home Secretary agreed to look at the classification of drugs. Would it not be sensible if all this were done together, rather than in a piecemeal fashion?
Mr Coaker: We are trying to move forward with a coherent drugs strategy. No decision has been made as to how we move forward with respect to the review of the classification system. The Home Secretary has yet to make a decision on how we proceed with that. We are required by the Drugs Act to come to a decision about determining the thresholds at which we have to presume it is supply. There has been widespread consultation on that. With respect to cannabis, you will know that that was recently confirmed as a Class C drug—although, I emphasise, an illegal drug. Whatever system you have in place, there will always be issues which arise with respect to this. There will always be people who have opinions about what should happen—quite rightly, because it is a very important and serious matter—but there will be people who will argue and disagree about different aspects of it. We have a drugs strategy; we are moving forward on it, and we are taking decisions as and when appropriate.

Q1254 Dr Iddon: However, I think you would agree with me that the worst thing we can do is to confuse the public, and particularly the young people in the public.
Mr Coaker: With my background, I know how particularly important that is. I think it is very important for us to say from this Committee that, whatever the arguments there were about cannabis, it remains an illegal drug. That is the message we have been putting out from the Home Office. That is the message that I have continued to put out in the various road shows I have been to and will continue to go to; and that is the message that I will continue to push.

Q1255 Dr Iddon: What evidence do you or the Home Office have that led you to classify magic mushrooms as some of the most dangerous substances, aligned with cocaine and heroin? They are not addictive, of course.
Mr Coaker: The whole debate about magic mushrooms was really not with respect to classification; it was trying to clarify the law, and that is why it was changed in the Drugs Act. You know that psilocin, which is the active ingredient, is a Class A drug; but the problem with it was within fresh or natural mushrooms. We saw a huge increase in the number of people who were importing magic mushrooms into the country. There was a big increase in that. There was therefore a concern that there was a loophole in the law with respect to psilocin being got—for want of a better way of putting it—through this loophole. People were able to get psilocin through this loophole. We felt it important therefore, since psilocin is a Class A drug—and there was clearly a problem out there, there was a huge increase in the import of it—for us to take action. So we saw it as a clarification of the law rather than any classification change.

Q1256 Dr Iddon: We seem to have agreement between the Committee and yourself this morning that classification according to the ABC system is according to harm—50% harm to the individual, 50% harm to the society. That is what the ACMD have told us. If that is the case, psilocin and psilocybin are not sold in shops and are not available on the street. I have not met anybody in my capacity as chairman of the Misuse of Drugs Group who uses them. I do not know a single person who has been harmed by them. Why are psilocin and psilocybin therefore in Class A?
Mr Coaker: Because that is the advice: that they were powerful hallucinogenic drugs, and that is why they were categorised with respect to that.

Q1257 Chairman: But we are supposed to have an evidence-based policy. That is the point that Brian is making. There is no evidence at all to show that these have the degree of harm which should put them into Class A.
Mr Coaker: What we are saying is that, should they be used, they are harmful drugs. They are Class A on the basis of the harm that they would cause were they to be used. We saw huge increases in the numbers of magic mushrooms which were being imported—naturally grown mushrooms, which were outside of the law—which would suggest that, if they were being imported in increasing numbers, somebody out there was using them, because people would be bringing them in to—

Q1258 Chairman: There is absolutely no evidence about that.
Mr Coaker: The police were saying to us that clearly, if you have this increase in imported magic mushrooms, they are being imported for a purpose. The law with respect to psilocin is that it is a Class A drug. We were worried that this was a loophole and we have closed that loophole. On the basis of clarifying the law—as was made in one of the court judgments in 2004, somewhere in Gloucestershire I think it was, in Gloucester Crown Court—we were asked to do that, which is what we did.

Q1259 Dr Iddon: You have moved drugs up and down this classification. Bob is going to come to one that you have moved up. You have moved cannabis down. Why has nobody looked at psilocin and psilocybin in the classification, decided that they are not causing harm to society or individuals, and moved them down? In which case, magic mushrooms would not be in Class A with a maximum penalty of 14 years' jail.
Mr Coaker: The opportunity for drugs to be looked at will always be there, and that issue is there; but at the current time there are no plans to reclassify it. Those drugs are Class A drugs. No doubt people will have heard what you have had to say this morning and consider the evidence; but, as I say, that is where they are at the moment. There was a loophole in the law which we wanted to close.

Q1260 Dr Iddon: My final question is this. Can you cite another example of where the Home Office have moved a drug around in the classification system merely to clarify the law, instead of looking at the harm?
Mr Coaker: I may have to write to you on that one.

Q1261 Bob Spink: Minister, will methylamphetamine be reclassified as a Class A drug today?
Mr Coaker: The announcement that we are making from the Home Office today is that—subject to the proper procedures of the House, because obviously it has to go through the process—it is our intention to reclassify methylamphetamine from a B to an A.

Q1262 Bob Spink: I congratulate you on that. I think that early action on this drug—because it is not too prevalent in the UK yet—will protect individuals and society. It shows that the system is working in this case, and a certain sensitivity towards this very harmful and dangerous drug. So I thank you for that. I am delighted with it. The ACMD said last week that they had made this recommendation to you based on, for instance, evidence from the police forces that the police had found an increasing number of laboratories manufacturing that drug. Is that so?
Mr Coaker: Can I start by saying that I was at the debate a few weeks ago when the Honourable Member raised this whole issue—as a Whip at that time. I think it does show that Parliament listens. I would like to thank him for the comments that he made at the beginning. It just shows that sometimes these things can work. It is the case that, in the letter that we received from the ACMD—and this is one of the reasons why the ACMD changed its advice—they had become aware of a small number of illicit laboratories for synthesising this substance. It was a low number but, yes, that was one of the things.

Q1263 Bob Spink: That shows the police actually initiating action within the ACMD, which is contrary to the other evidence that we have received from the Association of Chief Police Officers. I just wanted to get that on record. The ACMD have previously given evidence to us that increasing the classification of the drug would increase its kudos and therefore increase its use. That is why they were not considering that at an earlier time. I accept totally that people change views as situations change, and you change your decisions—especially a marginal decision, as it clearly was. Do you accept that there is this tension and that increasing the classification of a drug might increase its kudos and use?
Mr Coaker: These are judgments, and very serious judgments, that are made. Bob himself thought that it was important that the drug was reclassified from B to A. Why was that? Because, listening to the points that he put, they are exactly the same as the points which the ACMD put. Although low use at the current time—and I think it is important to emphasise from this Committee that there is not an explosion of use at the present time, but there is low use—the potential for harm was there. That is why Bob, others, and the ACMD said that there was therefore a need to reclassify it to an A.

Q1264 Bob Spink: Why did the ACMD announce this last week, and why did they choose the *Guardian* to announce it to?
Mr Coaker: I cannot comment on how it got in the *Guardian*. I do not think that was chosen. We can speculate on why things happen. I will just leave that with the Honourable Member.

Q1265 Bob Spink: It appeared on the front page of the *Guardian*.
Mr Coaker: I know where it appeared. I am just saying that the route was not entirely clear to me.

Q1266 Bob Spink: Do you think it appropriate that the ACMD should have its deliberations often in secret, and its advice to ministers often in secret, but selectively to release certain decisions to instruments like the *Guardian*, which they selected very carefully?
Mr Coaker: We have a close relationship with the ACMD and that is based on trust. It is based on close co-operation. I have only been in the job, as you know, four or five weeks. I am trying to come to terms with that. I have every confidence in the ACMD, in the work that they do. How that appeared in the *Guardian*, I am not sure. I am not blaming anyone for it. All I am saying is that, at the end of the day, however it appeared, we are pleased to say that we accept the advice that the ACMD have given us.

Q1267 Bob Spink: Does the Government intend to ask the ACMD to look at the classification of Ecstasy?
Mr Coaker: We have no plans to do that, no, at the present time.

Q1268 Bob Spink: Have you considered the evidence surrounding the classification of Ecstasy and the arguments for looking at reclassification?
Mr Coaker: My understanding is that there was some research done 10 years ago with respect to that, which showed that there were considerable harms out there. We also know that, if you turn it round, there is no research out there saying that it should be reclassified.
Bob Spink: That is a very good answer. I am sure that Leah Betts' parents will be delighted to hear it.

Q1269 Dr Harris: If you do not ask, you will never know. So if the Home Affairs Committee and the Runciman Report say there is a good case to move it from A to B, and if you are so confident that there is no research—and I have to say, given—
Mr Coaker: As far as I am aware.

Q1270 Dr Harris: . . . how much you know about the evidence base, or how much we all know about the evidence base as politicians, is questionable—what harm is there is asking the ACMD? Is this not just a case of "see no evil, hear no evil"? You do not want to ask something that you do not want to hear the answer to?
Mr Coaker: Not at all. We have no plans to reclassify Ecstasy. As Brian said, we regard it as a dangerous drug, and it is something we want to make clear to people that we see as potentially harmful. Because I thought that this may come up, I looked at some of the figures in terms of deaths where Ecstasy was actually mentioned on the death certificate. There were 48 in 2004; 33 in 2003; 55 in 2002, and so on.

Q1271 Dr Harris: Thousands in the case of heroin. Professor Blakemore said, ". . . on the basis of present evidence Ecstasy should not be a Class A drug. It is at the bottom of the scale of harm".
Mr Coaker: That is not the Government's view. The Government's view is that it is a harmful drug and we do not want to see it reclassified.

Q1272 Dr Harris: I know that you do not want to, but why do you not ask the ACMD to look at the evidence? They may reject the evidence.
Mr Coaker: The ACMD may come forward and look at that but at the current time, so far as I am aware, there are no plans for them to do so.

Q1273 Dr Turner: We can get off drugs now! I want to ask you both a much more general question. This Committee has in the past been critical of the Home Office for a lack of a scientific culture. That criticism has been mirrored by outside bodies. Do you think yourselves that the Home Office has sufficient expertise within it to be an intelligent customer for scientific and technological advice? If not, what are you doing to correct that?
Mr Coaker: Yes, there are a lot of committees and bodies now which have been set up: people responsible for considering the scientific evidence that comes in. On a general point, however, can I say this? The whole point and purpose of the Select

Committee system is to challenge the Government; it is to cause the Government to think. It has been a robust and interesting exchange of views that we have had here today. It would be arrogant for me, as a Home Office minister, to say that, whatever this Committee comes up with and makes as its recommendations, the Government would not need to go back and look to see whether it can learn from it. All I can say is that there are people responsible for evaluating the scientific evidence and research in the Home Office. Does that mean that we cannot learn from what the Committee may or may not say in its report? No, of course it does not. We will have to take that on board and listen to what is said—and we will do that.

Joan Ryan: Could I add to that? In the light of previous criticism, to be fair to the Home Office, we have to acknowledge the work that has been done to improve the level of scientific work, advice, expertise and experience within the Home Office. That is why I talked earlier about the Home Office science and innovation strategy. I particularly refer to the Science Research Group, which brought together several scientific units dealing with issues that cut across the Home Office and which were previously spread across Home Office departments. I think that this has significantly strengthened the science expertise availability and advice within the Home Office. I think that the use and extent of scientific expertise have grown substantially. From my own experience of the past four and half weeks, I can tell the Committee—as you know, I have responsibility for Forensic Science, for the DNA database, for licensing animal experiments, as well as all the identity scheme management issues and the science involved in all of those issues—I have never been exposed to so much science in my life, since I was about 15. I am very impressed with the clarity, the standard, the research, their ability to communicate all of that and their willingness to do so, and the amount of briefing that I receive. So from that point of view, yes, I think that they have made big efforts within the department and, personally, I am impressed with the scientific support that I am receiving in my role.

Q1274 Dr Turner: That is good to hear, though we are still in receipt of criticisms, and quite recent criticisms: notably, an academic who undertook research for the Home Office recently. To quote him, he said, "To participate in Home Office research is to endorse a biased agenda". Do you think that is fair?

Mr Coaker: No.

Q1275 Dr Turner: How do you protect research and evaluation from political pressures in the Home Office?

Joan Ryan: How do we . . .?

Q1276 Dr Turner: Protect research and evaluation from political pressure? How do you stop evidence being selectively used to back whatever preconception you start with?

Joan Ryan: We do not just use science internally; we do commission research and development that underpins policy development. I think that there will always be individuals who have a variety of views, for a variety of reasons. Overall, looking at the expertise both inside the Home Office and the expertise they commission for the R&D from outside the Home Office, I think that there is a good balance there and a degree of independence that is reassuring. I think that the co-ordination with other government departments through the Chief Scientific Adviser's committee is also a very good example of pulling together science and research across departments and looking at this—not embedded within the department but in a cross-departmental way. So we have both: embedded science and cross-departmental science.

Q1277 Dr Turner: Do you agree that there is still a potential trap that, instead of doing what the Government professes to do, which is to make evidence-based policy, you can actually be doing evidence-informed policy, which is subtly different?

Mr Coaker: The evidence will come up. There is an attempt, and a very serious attempt, by the Home Office to give scientific evidence much more focus within the department. Various groups have been set up, as Joan has just been saying; various attempts to give a greater strategic direction to all of that. Part of that is to inform and advise us about the best way forward with respect to the policies that we pursue. Inevitably, people will make judgments about policy decisions. That is what we all do all of the time. However, what we want is frank and open information on which we base the decisions, and an informed scientific base, where appropriate, to the decisions that we make—and that is what we are trying to do.

Q1278 Dr Turner: How do you see the role of the departmental Chief Scientific Adviser? Has he made an impact on the department, and how do you interact with him?

Joan Ryan: Yes, I have now met with him on a number of occasions. I think that there is an impact there. He has a dual role: that of an adviser and a manager. He has a clear remit to ensure improvement in quality standards; better evaluation of policies; improvement in internal skills by increased training and professional development. For the Home Office, that means he has a lead role in taking forward those reforms and bringing together the statistics, social and physical sciences. An example of that might be the DNA use, for instance. He is increasing the range of social science work, which we think is important—for example, on issues like immigration—and increasing science work across the Home Office portfolio beyond policing. So we need continually to monitor that that is having an impact, but I think that, in his role and the lead he is taking, he is taking things forward. It is very much in line with some of the comments that you have been making this morning about your concerns and previous criticisms.

Q1279 Dr Turner: What do you see as the main benefit of having the Chief Scientific Adviser in the Home Office?
Mr Coaker: Again, I think it goes back to the point that you made before: that we are trying to make informed policy decisions. Inevitably there will be judgments about that.

Q1280 Dr Turner: But you said to inform, rather than evidence based.
Mr Coaker: Your decisions are informed by the evidence. The evidence is there. You need to be informed by the evidence. In the end, however, people make judgments. Sometimes the evidence conflicts, even from scientists. You get different scientists saying different things. Then what do you do? They are both saying that they have the right evidence. "I am a scientist. I have this evidence." Another scientist comes along with completely different evidence. In the end, there is a judgment that is made; but what you are trying to do is that your policy is informed by the evidence. That is the role of the Chief Scientific Adviser.

Q1281 Dr Harris: In an article in *Criminal Justice Matters*, Professor Tim Hope, who is Professor of Criminology at the University of Keele, said, ". . . it was with sadness and regret"—in dealing with the Home Office—"that I saw our work ill-used and our faith in government's use of evidence traduced". My question to you is this. Do you take allegations like that seriously, or do you think it is just not fair and can never happen? That was the impression I had from your answer to the earlier quote, "To participate in Home Office research is to endorse a biased agenda". Are you concerned about allegations like that, or is it just mischief-making in your view?
Mr Coaker: No. If people are making comments to you, you need to take those comments into account, even if you find them uncomfortable. You need to listen to what people have to say. The point I was making before was that sometimes you will get conflicting pieces of evidence, in that some people will put forward one thing and somebody else will make a completely different point. In the end, you have to make a judgment.

Q1282 Dr Harris: This is a different point. This is an allegation of misuse, a traducement, bad faith by the Home Office. It is a separate issue about whether the policy was right. My question is this. Are you sensitive to that?
Joan Ryan: There are a large number of people who say very complimentary things as well. So there is always a balance to be struck. It is true that different scientists take different views.

Q1283 Chairman: But you agree that they should be taken into account?
Mr Coaker: You do. They should always be looked at and taken into account. I am sorry if I gave the impression before that I did not, because I did not mean that—if I did give that impression.
Chairman: Vernon Coaker, Joan Ryan, thank you very much indeed. It has been a long session. We have enjoyed it enormously. It has been very valuable to us.

Written evidence

APPENDIX 1

Memorandum from the Government

1. Scientific Advice, Risk and Evidence in the Identity Cards Programme

This section covers the mechanisms by which conclusions are arrived at and the external sources of evidence and guidance used by the Identity Cards team. It will also explain how these data and the conclusions drawn from them are presented to the programme's assurance groups and to ministers.

Risks relating to biometrics

1.1 Biometrics is a key technology underpinning the delivery of the programme's aims (although it should be noted that the scheme's integrity is not wholly dependent on biometrics because of the biographical or "footprint" checks which will be made on applicants) and so examples on the use of scientific evidence in the Identity Cards programme will be drawn from this area.

1.2 Some biometrics technology is relatively immature and the whole field is fast-moving. The programme anticipates a biometric scheme comparable to the few, large-scale deployments which currently exist there is a necessity to base our models of the likely performance of the biometric technology on the best scientific evidence. Further, because it is a key dependency, it is necessary to have the best possible assurance of the work done on biometrics and also to ensure that the risks and the potential of biometrics are properly communicated to ministers.

1.3 The uncertainties over biometric technology and thus those areas which need most attention are encapsulated in several key risks associated with biometrics. These are summarised below:

— It may be impossible to prevent applicants falsifying (spoofing) their biometrics. This risk can be mitigated through analysing the threat posed and designing the correct detection processes and by ensuring that the deterrent regime is appropriate.

— The matching of newly enrolled biometrics against all those already enrolled may not be 100% reliable, raising the risk that a very small number of people may be able to enrol more than once without authorisation[1]. Likewise, the matching of an individual's fingerprint or iris against their previously enrolled biometrics in order to verify their identity may not always be reliable. Mitigation of these risks requires modelling the likely distribution of, and the mechanisms behind, these mismatches and then looking at the impact on stakeholders and modelling the ways in which these mismatches will be detected by other, non-biometric, means.

1.4 Within the context of these risks, key requirements of the biometrics need to be set:

— Which biometrics should the scheme use, and will these be sufficient to meet the performance demands of the scheme?

— What are the criteria and tests we should apply to biometric technology suppliers?

1.5 It is not necessary for the purposes of the programme to embark on publicly-funded scientific research to improve the capabilities of biometrics. Our approach to answering these questions has focused on gathering the best evidence available from existing programmes, academia and suppliers, and on using trials to answer specific questions for which data are not available.

Sources of evidence, advice and assurance

1.6 We undertook a comprehensive survey of the academic and commercial literature on biometrics, and the published reports available from existing biometric schemes, government laboratories and standards bodies.

1.7 In 2003 NPL undertook a feasibility study for us on the use of biometrics in a national identity card scheme. One of the recommendations of this report was the trial we ran in 2004 to gather evidence on public perceptions and attitudes towards biometrics and data on the timings of biometric recording and verification processes. This was conducted with UKPS and demonstrated that the overall experience was positive and met or exceeded the expectations of a vast majority of people. It provided some findings on the technology, but was not an assessment of the technological capabilities of biometrics.

[1] There will be exceptional circumstances (eg for the purposes of Witness Protection) under which people will be permitted to enrol more than one identity.

1.8 We are currently funding technical work at NPL to define a methodology to assess the interoperability of fingerprint systems using systems from the four leading fingerprint identifications systems. We are planning a set of trials for 2006 which will look at the relative performance of suppliers' integrated biometric systems in the areas of timing, usability and spoofing-resistance, and the relative performance of suppliers' matching algorithms on a "test" database of biometric records.

1.9 We are working with leading biometric experts from:

— US National Institute for Standards & Technology.
— San Jose University.
— UK National Physical Laboratory.
— Members of the Biometrics Working Group.
— Communications-Electronic Security Group (part of GCHQ) and other experts in the field of fraudulent use of biometrics.

1.10 We are learning from the experiences of our colleagues from:

— UK Passport Service (UKPS).
— Immigration & Nationality Directorate (IND).
— Police Information Technology Organisation (PITO).
— International Biometric Identity Cards Schemes such as Hong Kong & the Philippines.

1.11 We have consulted with leading biometric technology firms in industry:

— The Identity Card Programme has met with 15 companies involved with biometrics and is currently undertaking further market sounding activity in relation to biometric matching performance. This contact has taken place in accordance with OGC (Office of Government Commerce) procurement rules.

1.12 We receive assurance on biometrics from a number of sources, principally:

— We have given evidence on biometrics on two occasions to the Home Office Science and Technology Reference Group (chaired by the Permanent Secretary).

1.13 The government's Biometrics Assurance Group and the Home Office Senior Biometric Advisor will review biometric aspects of the Identity Cards Programme.

— Sir David King, the Government's Chief Scientific Adviser, chairs the Biometrics Assurance Group which has been established as a panel of internationally eminent specialists in biometrics and related technologies.

1.14 Scientific evidence and its meaning for the programme and the output from the programme's assurance bodies are presented to ministers via submissions and face-to-face briefings. Numerical data is frequently presented (eg the current measured levels of passport fraud as a percentage of applications and the anticipated reduction as a result of the introduction of biometrics) as are comparisons with other schemes (both those in other countries such as the US, the UAE, the Netherlands, Hong Kong, the Philippines and Germany and also relevant schemes in the UK such as IDENT1, the Police fingerprint database).

January 2006

APPENDIX 2

Supplementary memorandum from the Government

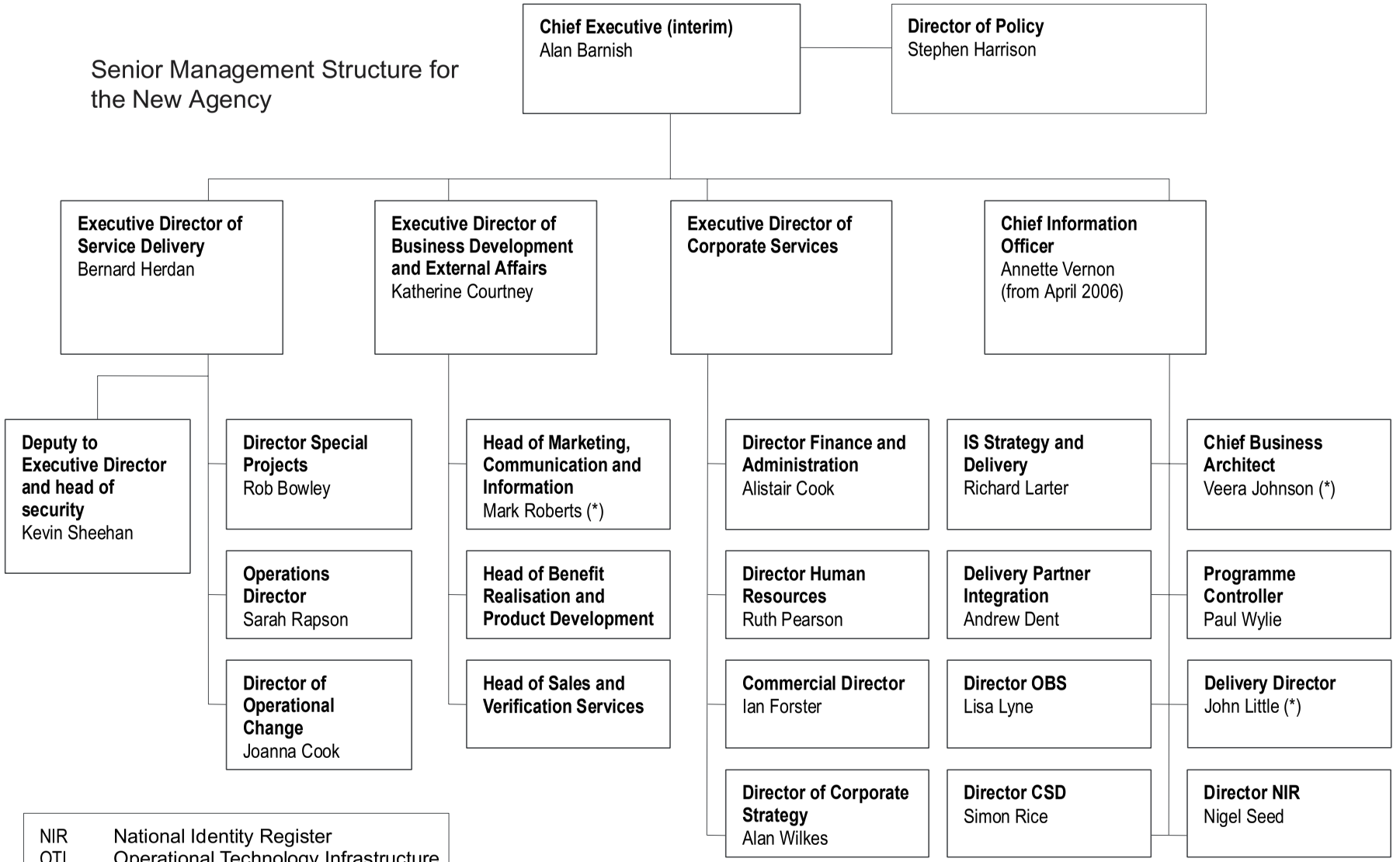
STRUCTURE OF IDENTITY CARDS PROGRAMME

Assuming the Identity Cards Bill has received Royal Assent, the Identity Cards Programme and UKPS (UK Passport Service) will combine to form a new agency on 1 April 2006. This will be headed by a new chief executive who will be recruited by open competition following Royal Assent of the Bill. There will be four executive directors responsible for service delivery, business development, corporate services, and the Chief Information Officer (CIO). The procurement of the components of the ID Cards scheme mainly falls within the CIO's brief.

As of February 2006 there were 186 people working with the Identity Cards Programme team. This comprises 54 civil servants and 98 consultants from our development partners and 34 interims.

The diagram on the following page shows the combined high-level structure of the Identity Cards Programme and UKPS as they form a new agency.

Senior Management Structure for the New Agency



NIR	National Identity Register
OTI	Operational Technology Infrastructure
OBS	Operational Business Services
CSD	Corporate Support Development
(*)	PA Consulting

2. Academic and Commercial Survey

In this section and in others some terms are used to describe the performance of biometric systems in matching a biometric with previously recorded biometrics. Below is an explanation of the most commonly used terms:

- False Match Rate (FMR): the probability that a biometric sample, when compared with a biometric of the same type from a different (and randomly-selected) individual, will be falsely declared to match that biometric. Eg a false match would be where your fingerprints match another inividual's.
- False Accept Rate (FAR): the probability of a biometric matching transaction resulting in a wrongful confirmation of claim of identity (in a positive ID system—ie one which tests a claim that a person is enrolled in a system) or non-identity (in a negative ID system—ie one which tests a claim that person is not enrolled in a system). A transaction may consist of one or more wrongful attempts dependent upon system policy. Eg a false accept would be where your fingerprints match someone else's in a database of fingerprints.
- False Non-Match Rate (FNMR) (or False Reject Rate—FRR): the probability that a biometric sample, when compared with a biometric of the same type from the same user, will be falsely declared not to match that biometric. Eg a false non-match would be where your fingerprints fail to match your previously enrolled fingerprints
- False Reject Rate (FRR): the probability of a biometric matching transaction resulting in a wrongful denial of claim of identity (in a positive ID system) or non-identity (in a negative ID system). A transaction may consist of one or more truthful attempts dependent upon system policy. Eg a false reject would be where your fingerprints fail to match your own in a database of fingerprints
- Failure To Enrol Rate (FTE): the expected proportion of the population for whom the system is unable to generate repeatable biometrics. This will include those unable to present the required biometric feature, those unable to produce an image of sufficient quality at enrolment, and those who cannot reliably match their Reference in attempts to confirm the enrolment is usable.
- Failure To Acquire Rate (FTA): the expected proportion of transactions for which the system is unable to capture or locate an image or signal of sufficient quality.

Different biometrics (eg fingerprint, iris, face) will have different performance characteristics and these will vary between different implementations of a single type of biometric and will also vary dependent on how the system is designed and operated (eg it will vary with the competence and experience of operators).

On the next page are extracts taken from the document "Biometric and Card Technology Options", produced during September 2004. The section summarises the work done to survey the academic and commercial literature on biometrics. This document was not shown to ministers—rather it was a resource for officials so that they could have in one place a summary of relevant research.

An important point to note when reading this work is that where the performance of biometric systems is discussed, this is the "raw" performance of individual biometric technologies measured by standards institutions and academic bodies. It does not necessarily equate to the performance of a biometric system which combines several biometrics or which allows multiple attempts at enrolling a biometric. Nor does it equate to the performance of an end-to-end enrolment system which uses biometrics as a single component of identity validation together with, for example a biographical check and an interview.

To further inform the committee about the subject we have included as a footnote on p 17 a short note on biometric spoofing. This was part of a summary on biometrics that Baroness Scotland provided for Peers following the first 3 days of Committee in the Lords on 11 December 2005.

2. Biometric Technology Options

2.1 *Scope*

This document considers the performance of the biometric sub-system and the capabilities of card technology. It covers only the technical performance of the biometric capture device, template generation and matching algorithm. It does not address any IT aspects of the biometric sub-system, for example the National Identity Register database.

A biometric system has traditionally consisted of three subsystems:

- Image acquisition.
- Feature extraction.
- Matching.

In image acquisition, a digital image of a biometric is recorded either from a live scan of a person's biometric or from an impression of a person's biometric on paper (eg fingerprint cards). Feature extraction is the process of representing the captured image in some space (the "template") to facilitate matching. Matching involves computing the likelihood of the biometric coming from subjects (persons) in the database. The performance of the whole system depends on how well each subset behaves.

The biometric capture device is the hardware that captures an electronic representation of the biometric (eg an iris camera or a fingerprint scanner). The template generation algorithm processes the captured image into a template and the matching algorithm computes the probability that a template matches another.

2.2 *Biometric performance definition and terms*

There is no standardised method for presenting biometric performance or even for the terms used to describe performance. Common terms used are FMR, FAR, FNMR, FRR, and FTE. FMR, FNMR and FTE are the properties that are least ambiguous. This document uses definitions in [ref NPL testing report]. In particular we make reference to the following:

- FMR—this is defined as the probability that the biometric sub-system will decide that two biometric templates are from the same individual when in fact they are not.
- FNMR—this is defined as the probability that the biometric sub-system will decide that two biometric templates are not from the same individual when in fact they are.
- FTER—this is the percentage of failures to enrol in the biometric system ie it is the percentage of people who cannot give a biometric of sufficient quality to be enrolled.

In the context of databases (of size N) frequently confused terms are FAR, FMR and effective FMR. In this document we define these, for positive identification scenarios as:

- FAR or Effective FMR $\approx$ N*FMR (assuming N*FMR $<<$ 1)
- FRR = FNMR
- TAR = 1-FRR

FAR is larger than FMR as the more times a match is attempted the more matches will result. FRR can be thought of in terms that a person's only true match is against their own template.

Other terminology and definitions used to describe biometrics and biometric performance testing are set out in Appendix E.

In term of interpreting statistics:

- An FAR of 1% or 0.01 in an enrolment (identification) scenario implies that every hundredth enrolee will falsely match against the enrolment database. In a verification scenario (e.g. against a template stored on a card) a person would have to acquire 100 cards before they could falsely match against one.
- An FRR of 1% or 0.01 in an enrolment (identification) scenario implies that an imposter would have to try 100 times to re-enrol under a second identity. In a verification scenario (e.g. against a template stored on a card) a person would be refused entry to a building at every hundredth attempt.

FMR can be derived from FAR statistics generated during trials using the equations above. However, this FMR should not really be used to extrapolate an FAR beyond the database size that was used to calculate it in the first place. For example if FAR of 0.5% is measured using a database of 10 million, then the FMR is 5e-10. The "estimated" FAR for a database of 100 million is therefore calculated at 5%—this is a result that has not been tested.

2.3 *Biometric performance in large scale tests*

The most widely independently tested biometrics (in terms of database sizes) are:

- Finger (millions)
- Face (10,000's).

Iris performance statistics from independent tests are limited to 100's. It should be noted that there is iris vendor supplied limited data based on database sizes of 100,000's gathered from a real life deployment. There is no large scale database for multimodal biometrics (two or more distinct biometrics captured under the same controlled conditions) although there is large scale multibiometric (1–10 fingers) data.

Principal tests have been conducted by NIST and to a lesser extent NPL and the FVC competitions in Italy using databases gathered from real life deployments tested against vendors' products under test conditions.

There is very little data from real life deployments in the public domain.

As mentioned previously there is no standard test protocol. As heavy use is made of NIST data the NIST protocol is detailed below.

There are three distinct test scenarios that NIST defines which are called Verification, Closed-Set Identification, and or Open-Set Identification. For each task, appropriate performance statistics are defined.

— In verification (1:1 matching), a subject presents his biometric image to the system and claims to be a person in the system's gallery. For evaluation, each probe image is compared to each gallery image independently. Two performance measures are computed: True Accept Rate (TAR), the fraction of true identity claims scoring above a threshold; and False Accept rate (FAR), the fraction of false identity claims scoring above threshold. The resulting relationship between TAR and FAR, where each point is defined as a function of score threshold, may be graphed on a Receiver Operator Characteristic (ROC) curve.

— In closed-set identification (1:N matching), only subjects known to be in the gallery are searched. The system's ability to identify the subject is evaluated based on the fraction of searches in which the probe image scored at rank k or higher. A probe has rank k if the correct match is the kth largest similarity score. No score threshold is used. The relationship between Identification rate and rank may be graphed on a Cumulative Match Characteristic (CMC) curve.

— In open-set identification1 (1:N matching), each subject is searched against the gallery, and an alarm is raised if the subject occurs in the gallery. A subject is considered to be "in the gallery" if the probe image scored above the threshold at rank k or higher. In evaluation, the system's ability to detect and identify is measured as two rates: the true accept rate and the false accept rate. An open-set identification ROC plots TAR vs. FAR. This may be generalized using rank, where the subject must be detected and identified at rank k or better.

Note that in a verification (1:1) task, the performance metrics are based on each comparison of a probe image to a gallery image, whereas in the identification (1:N) tasks, the performance metrics are based on each search of a probe image against the entire gallery.

The table below summarises biometric performance data from independent large scale tests:

Source	*Trial*	*Data source*	*Gallery*	*Probe*	*Type*	*Verification/ Identifications*	*Statistics*
NISTIR 7110	Matching performance for the US-VISIT IDENT system	operational—US VISIT	6000000	60000	finger—live index pairs	Identification	FAR 0.31% TAR 96%
NISTIR 7110	Matching performance for the US-VISIT IDENT system	operational—US VISIT	6000000	60000	finger—live index pairs	Identification	FAR 0.08% TAR 95%
NISTIR 7110	Matching performance for the US-VISIT IDENT system	operational—US VISIT	6000	6000	finger—live index pairs	Verification	FAR 0.1% TAR 99.5%
NISTIR 7123	FPVTE2003	operational—multisource	9000	4000	finger—10 live slap	Identification	FAR 1e-4 TAR >0.999
NISTIR 7123	FPVTE2003	operational—multisource	21119	4184	finger—2 live flat	Identification	FAR 1e-4 TAR 0.9959
NISTIR 7123	FPVTE2003	operational—multisource	3190	1204	finger—1 live flat	Identification	FAR 1e-4 TAR 0.9825
NISTIR6965	FRVT2002	operational—US Visa Services	37437	74874	face 2D	Verification	FAR 1% TAR 90% (indoors)
NISTIR6965	FRVT2002	operational—US Visa Services	37437	74874	face 2D	Verification	FAR 1% TAR 54% (outdoors)
NISTIR6965	FRVT2002	operational—US Visa Services	37437	74874	face 2D	Identification	Identification rate 73% at rank 1
X92A/4009309	Biometric Product Testing Final Report	scenario—NPL staff	200		iris	Verification	FTE 0.5% FMR 0% FNMR 1.9%

The table below summarises biometric performance data from Vendors etc:

Source	*Trial*	*Data source*	*Gallery (no of people)*	*Probe*	*Type*	*Verification/ Identifications*	*Statistics*
TR-02-004	Iridian Crossmatch study	operational composite datasource	120000	9000x17000 sets	iris	Verification	FAR 3.92e-6
International Airport Review, Issue 2, 2004	UAE border deployment	operational	430,000	2.2 million	iris	Identification	9,506 matches, none disputed, 0.2% FRR at third attempt
Manufacturer	"FRVT2002 test set up"	unknown	unknown	unknown	face 3D	Verification	FAR 0.1% FRR 1.5% to 3%
Manufacturer	"FRVT2002 test set up"	unknown	unknown	unknown	face 3D	Verification	FAR 1% FRR 0.5% to 1.5%
Phillipines ID	SSS-ID	Phillipines Government	7900000	unknown	finger—4 (2 on card, 4 on NIR)	NA	FTE $\geqslant$ 2% ("finger wound")
Cogent	Cogent study	Cogent database	10 million	25000	finger—2	Identification	FAR 0.5%, FNMR 5%
Cogent	Cogent study	Cogent database	10 million	25000	finger—4	Identification	FAR 0.1%, FNMR 1%

Source	*Trial*	*Data source*	*Gallery (no of people)*	*Probe*	*Type*	*Verification/ Identifications*	*Statistics*
Cogent	Cogent study	Cogent database	10 million	25000	finger—10	Identification	FAR 0.004%, FNMR 1%
ATOS Origin	UKPS	UKPS	up to 10,000	NA	iris	NA	FTE 9%
ATOS Origin	UKPS	UKPS	up to 10,000	NA	finger	NA	FTE 2%

In terms of summarising finger and face peformance, NIST highlights the following regarding the data above: These tables highlight the following points:

- One-to-Many Matching (Identification)—NIST recommends ten slap fingerprint images stored in type 14 ANSI/NIST-ITL 1-2000 formatted records for enrolment and checking of large databases. Face images are not recommended for identification applications. With available fingerprint scanning technology, the acquisition of 10 slap fingerprints should take only slightly more time than the acquisition of two flat fingerprints.
- One-to-One Matching (Verification)—NIST recommends one face and two index fingerprints for verification. All three biometrics should be in image form. The face image should conform to the ANSI/INCITS 385-2004 standard. The fingerprint images should conform to the ANSI/INCITS 381-2004 standard with 500 dots per inch (dpi) scan resolution.
- The two-fingerprint accuracy (or true accept rate (TAR)) at 0.1% false accept rate (FAR) for the US-VISIT two fingerprint matching system [4] is 99.6% while the best 2002 face recognition TAR at 1% FAR was 90% using controlled illumination. When outdoor illumination was used in 2002, the best TAR at 1% FAR was 54%. Even under controlled illumination, which is not currently used in US-VISIT, the error rate of face recognition is 25 times higher than the two-fingerprint results using US-VISIT data that has 10 times lower FAR. If the case of uncontrolled illumination is considered, this factor would be 115. This means that face recognition is useful only for those cases where fingerprints of adequate quality cannot be obtained.
- FTE for fingerprints from real life deployments are 2%, for iris it is between 0.5% and 9%.

In terms of iris data, although the performance is impressive, it should be noted that no independent testing on databases of millions has been undertaken to date. Iris recognition generates a template with a large sequence of bits for comparison (the iris code). This means that if the bit sequence from two irises are uncorrelated, the probability of the number of bits that match being significantly different from half of the total number of bits is very small indeed. This statistical argument is used by Iridian (the holder of iris IP) to argue for the superior performance of this biometric. The difficulty is that there is little evidence for the iris code being truly random (in the sense that there is no significant correlation between iris codes from different eyes).

2.4 *Multimodal biometrics*

As mentioned previously there is no large scale database for multimodal biometrics (two or more distinct biometrics captured under the same controlled conditions) although there is large scale multibiometric (1–10 fingers) data that has been discussed above.

There are no published data on the performance of multimodal systems that combine two iris patterns although there seem to be little correlation between the two irises of an individual. It is unclear whether combining these biometrics would significantly increase performance. The logic of the argument is as follows:

- Correlation effects eg some people are significantly worse (through physical characteristics or temperament) than the mean in their ability to supply a biometric.
- For this group of people the FNMR is (comparatively) very high
- Use of a second biometric does not greatly reduce the absolute value of the FNMR for these people

For example:

- Scenario 1 (random distribution of FNMR). In this idealistic scenario everyone is equally good (or bad) at producing a biometric. Everyone therefore has an equal chance of producing a FNM. If the probability of a FNM for this biometric is p and a second biometric with FNMR = q is used in combination then the combined FNMR is pq. For 2% FNMR this would imply that pq = 4x10-4.
- Scenario 2 (some people bad at presenting biometrics). Suppose that 90% of the population present excellent biometrics (FNMR $\geqslant$ 0) and the remainding 10% present poor biometrics (FNMR = 20%). The averaged FNMR is still 2% (0.2x0.1 + 0.9x0) = 2%. If however a second biometric is introduced then the FNMR for the 90% part of the population remains at $\geqslant$ 0 whilst the FNMR for the remaining 10% is now 0.2x0.2 = 0.04 and the mean FNMR is only reduced to 4x10-3 (0.1x0.04 + 0.9x0).

2.5 *Effect of image quality*

There is no standard measure of image quality for fingerprint, iris or face. Standards exist that specify

- Recording equipment (eg FBI Appendix F&G guidelines for fingerprint capture devices)
- Guidelines for facial images (illumination, size of image etc.)
- Compression techniques (JPEG, WSQ etc)

Recent work by NIST on image quality of fingerprints has shown that image quality has a large effect on performance statistics. [see NIST 7110, figure 12, p23, ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7110.pdf]

This study used US VISIT data and assigned a measure of 1 for best quality and 8 for worst quality. As can be seen performance for quality 1 to 3 (top three plots) is very similar.

Another study by NIST [NIST 7151] used NIST's own image quality assessment tool. This yielded similar conclusions. In this study image quality 1 was excellent and 5 was poor. In this report NIST developed a method to assess quality of a fingerprint that can forecast matcher performance. This included an objective method of evaluating quality of fingerprints. These image quality values were then tested on 300 different combinations of fingerprint images data and fingerprint matcher systems and found to predict matcher performance for all systems and datasets. The test results presented in the body of the report for US-VISIT POE data show that the method is highly accurate.

Automatically and consistently determining quality of a given biometric sample for identification and/or verification is a problem with far reaching applications. If one can determine low quality biometric samples, this information can be used to improve the acquisition of new data and also reduce FTE. This same quality measure can also be used to selectively improve archival biometric gallery by replacing poor quality biometric samples with better quality samples. Weights for multimodal biometric fusion can be selected to allow better quality biometric samples to dominate the fusion.

The definition of quality can also be applied to other biometric modalities and upon proper feature extraction can be used to assess quality of any mode of biometric samples.

Image quality of a biometric is a function of a number of factors, for example:

- Changes in the physical biometric
- Damage due to cuts, abrasion or other injury
- Changes due to ageing
- Changes due to reader;
- XY position of fingers on reader
- Angles of each finger tip relative to surface of reader
- Joint position causing changes in skin tension and stretching of skin
- Forces applied by finger in plane of reader surface stretching skin
- Torques applied by finger in plane of reader surface stretching skin
- Force applied by finger in Z direction compressing ridges to reduce contrast (pressure too high) or providing insufficient contact area (pressure to low)
- Sensitivity of reader to skin condition (moisture and skin oils)

Sensitivity of individual biometrics is discussed in the Biometric Types section.

Image quality is also a function of the capture equipment. The FBI has defined several criteria (FBI EFTS Appendix F and G) to evaluate fingerprint capture devices that can be used within its IAFIS system. These include signal to noise ratio, greyscale linearity, grey level uniformity etc. In general there does not appear to be much information as to how capture devices are kept in calibration in the field. This is particularly the case for other biometrics such as face and iris. Iridian approved iris cameras perform an on camera quality check before the Iriscode is generated on and sent from the camera.

2.6 *Matching speed*

Matching speeds are an issue for enrolment into large databases with a high rate of enrolment where identification is required. The likely timescale for processing the biometric confirmation has important implications:

- The process flow during the enrolment appointment, specifically the nature of the questions that could be asked at the post biometric capture interview
- The overall security of the system—on the one hand a view could be taken that an enrolment decision reached with the applicant present in the enrolment centre is likely to discourage attempts at repeat enrolment, on the other hand, it has been suggested that non real time matching will give an opportunity for extensive cross checking of applications and the option to inform the relevant agencies in cases of suspected fraud (the latter is the Security point of view).

— The nature (in terms of cost, complexity, size etc) of the matching hardware

Assumptions for calculating times based on fingerprint only:

— The time for the enrolment decision is based solely on matching speeds, implying that access to NIR database of templates will not be limiting

— Fingerprint matchers work at a rate of 1 x 1e9 matches/minute (ref supplier meeting) in the something with a fridge-freezer footprint

— Each person will enrol 10 fingerprints

— The NIR database of templates possesses 1 x 1e9 records (ie 1 x 1e6 enrolments with 10 fingerprints each)

— Enrolments take place at an average rate of 50,000 per day (based on UKPS peak rate in March 2004 was $\geqslant$30,000 per day (UKPS Annual Report, 2003–04)

— To allow for peak loading a scale up factor of 5 is used

— Enrolments take place over an 8h day (480 minutes)

— Matches take place over an 8h day

— Each match attempt involves 100% penetration of the database to eliminate potential binning errors

The calculations and rationale are set out below:

For real time matching, it is essential that the peak rate of enrolment applications does not exceed the rate of enrolment match results, otherwise a queue would build up.

This "no queuing stipulation" means that the matching capability of the system must equal peak demand over a reasonable time period. So given that up to 50,000 enrolment applications will take place per day, this could be averaged out to 100 enrolments per minute.

— Each application will involve 10 x 109 match attempts (10 fingerprints, each checked against a database of 1 x 109 records)

— Therefore the number of matches per minute will be 100 x 10 x 109, ie 1012

— Given that matchers work at a rate of 1 x 109 matches/minute, this implies that the system will need 1,000 matchers to keep up with peak demand.

Note that during any given time interval, it is possible that the maximum rate of enrolment applications could exceed the sustainable peak of 100 per minute. For example, 2 enrolment applications could arrive in a second. However, assuming that the enrolment appointments will be scheduled at 20 minutes intervals and that there will be 2000 enrolment booths , it will not be possible to sustain a peak enrolment rate above 100 per minute. Any transient increase over a short time period will inevitably be smoothed over a 20 minute time interval.

The maximum decision time is determined from the time required for a single matcher to check 1 person's fingerprints against the entire database

Since each enrolment application will involve 10 x 109 match attempts, and matchers work at a rate of 1 x 109 matches/minute, the match decision time for each applicant is 10 minutes. This is deemed to be the maximum matching time since applicant is allocated a single matcher to process the matching checks.

The minimum decision time is determined from the time required for a single matcher to check 1 person's fingerprints against the entire database divided by the number of matchers available per person

The maximum decision time of 10 minutes is based on using a single matcher per applicant. However, since it has been shown that 1,000 matchers will be required to avoid queue build up and that 100 enrolment applications will arrive per minute, it is feasible that each individual application could be divided amongst 10 matchers. This would give a minimum matching decision time of 1 minute. In this scenario, each matcher sees a portion of the total database (a 1/10th), whereas in the maximum decision time scenario, each matcher checks against the whole database.

Note that there might be design issues that suggest that one of these scenarios is more preferable, however for now the decision time for real time matching can be estimated to be between 1 and 10 minutes.

For non real time matching, a queue can be allowed to build up

Non real time matching allows matching checks to take place in intervals when enrolment is not taking place. Hence in the absence of fresh demand, a queue that had been built up can be eliminated. The length of the queue that can be allowed to build up depends on the ratio of time that enrolment centres are open to the enrolment downtime. Hence there are two options for non real time matching: 24 hour turnaround (where enrolments are processed at a rate of $\frac{1}{3}$ the application rate); and a 1 week turnaround (where enrolments are processed at a rate of $\frac{1}{4}$ the application rate).

However, the total number of matchers required is the product of the number of enrolments per unit time and the amount of time (in the same units) that a matcher spends on each enrolment. This stipulation prevents the build up of a queue of applicants, which could only be dealt with when enrolments were no longer occurring, ie in a scenario where enrolment decisions are not real time.

No. of enrolments per min = (enrolments per day) x (scale up factor) / (minutes per day) = 520 min-1

Time (minutes) required for 1 person to enrol 10 fingerprints using a single matcher: = (database size) x (no. fingerprints)/(matching speed) = 9.2 min

Number of matchers required = (matching time) x (no. of enrolments per minute) = 4784

Number of matchers available per person per minute (note –all 4784 matchers could be put on the job, giving a decision time of 0.12 secs or just 1 matcher giving 9.2 min, so the decision time varies between these extremes) = total number of matchers required/no. enrolments per min = 9.2

Decision time per enrolment = time required to enrol 10 fingerprints using a single matcher/number of matchers available per person = 1 min

For real time matching, the number of matchers required is a function of the peak enrolment rate and the time required for 1 matcher to search 1 set of records against the entire database. Once the number of matchers required is calculated, the average decision time can be calculated by dividing the time required for 1 matcher to search 1 set of records by the number of matchers available per person per unit time. Using the assumptions stated above, we have deduced that:

- 4,784 matchers will be required for fingerprint scanning
- Average decision time for each enrolment applicant is 1 min

Note that the number of matchers required is sensitive to the "peak scale up factor" and the number of enrolments per day. The former has been estimated at 5 for illustrative purposes, but modelling of likely demand forecasts would provide a more realistic number. Note also that the costs of real time biometric decision ($\geqslant$5000 match engines), should be set against the benefits (improved security, simpler processes). We could assess the options of doing this against overnight batch type matching (the cost being 1,594 matchers, keeping other assumptions the same).

Note also that iris matching not included in this analysis. As stated previously no Iris database of millions is known to exist. Iridian matchers run at a rate of 0.5 million to 1 million matches per second per server.

The speed at which matching can be achieved is also dependent on the algorithm type. For the US IDENT system a thoughput of 1,035,000 matches per second was achieved, although special purpose hardware is required and some filtering is used to reduce the number of fingerprints that need to be examined in detail. Without filtering a figure of 734,000 matches per second was achieved. In general minutiae based templates have a higher match rate pattern based ones.

Matching speeds for verification scenarios are generally not an issue. Matching can occur on the card, in the card reader or on the database. In each case only one pair of records is being matched.

2.7 *Spoofing*

Spoofing is the practice of substituting a false biometric in place of the real one[2]. It is normally attempted by the following approaches:

1. Re-activating a latent image from a previous enrolment
2. Use of a false biometric—impressions in a compliant material e.g polymer coatings on a finger [ref], pictures of irises on false eyes [ref]
3. Use of a biometric from another individual (alive or dead)

[2] *Letter to Peers after Lords Committee:* Can biometrics be forged or "spoofed"?
Studies have shown that biometrics can be "spoofed" to fool a biometric reader. However, once more, this must be placed in context. These studies, often conducted in laboratory conditions, only sought to see if it were possible and did not attempt to see it would be possible to conceal such attempts if you were attempting to nrol or verify biometrics in the prescence of a trained operator. That is a very different undertaking.
In practice, it would be very difficult to spoof biometrics in front of a trained operator who uses technology that incorporates "liveness detection" measures, which identify if the biometric presented is an actual biometric or, in fact, an attempt to copy a biometric. Such studies also do not consider the fact such attempts would also encounter the other non-biometric security measures which have been previously mentioned.
The Identity Cards Programme is also working to improve current methods to prevent spoofing with established experts from the Communications Electronics Security Group (CESG), the National Physical Laboratory and independent specialists. Resistance against spoofing will also form part of biometric testing of any technologies procured.

2.8 *Types of Biometrics*

This section outlines the most widely used, or most widely discussed biometrics, namely:

— Fingerprint
— Face
— Iris
— Signature

For each of these biometrics, a brief overview is given of the characteristics that are measured, devices used to capture the biometric and features that are extracted together with the some of the key advantages and disadvantages of these systems. Later sections describe some other biometrics technology methods that are also available but are less proven by large scale testing.

2.8.1 *Fingerprint*

Fingerprint recognition is one of the best known biometric techniques, because of its widespread application in forensic sciences and law enforcement. Fingerprints are one of the few biometrics that can be "left behind" and therefore gathered in a person's absence.

The basic characteristics of fingerprints do not change and are usable beyond a given age (12 years [ref Cogent]. Fingerprints are however susceptible to wear and damage due to: occupation, hobbies, injury, burns, disease etc.

Fingerprint technology is widely established—Fingerprints have long been associated with law enforcement and commercial automated fingerprint identification systems (AFIS) have been available since the early 1970's. Current applications of fingerprint biometrics include:

— Criminal and civil AFIS
— Physical and logical access
— Fraud prevention in entitlement programmes

A variation on fingerprint verification is "palm print" verification which relies on physical features of the palm including line features, wrinkle features, delta point and minutia features. Palm print is not as widely tested as fingerprint.

Fingerprint Acquisition Characteristics

A fingerprint is a complex combination of patterns formed by ridges. The Henry system derives from the pattern of ridges; concentrically patterning the hands, toes, feet and in this case, fingers (patterns are called arches, loops and whorls). The most distinctive characteristics are the minutiae, the smallest details found in the ridge endings and bifurcations (where a ridge splits into two). Most fingerprint identification systems rely on the hypothesis that the uniqueness of fingerprints is captured by these local ridge structures and their spatial distributions.

Fingerprint technology uses the impressions made by the unique ridge formations or patterns found on the fingertips. Livescan technologies use "frustrated total internal reflection" to capture details of distinct ridges on fingertips in a digital image. A clean finger is placed on a coated platen that is typically glass or hard plastic and light is scanned across the platen from below. Where a ridge is present and close contact with the platen is obtained, the light rays do not exit the top of the platen and are scattered back into the platen and onto a detector. Where a valley is present, the light is reflected in a focussed ray and a strong signal is detected (refs 2, 3, 4). In most optical devices, a charged coupled device converts this image of dark ridges and bright valleys into a digital signal. Thus a high contrast binary imaged is produced by taking the average grey level pixel and processing every single pixel above this level as a binary "one". Every pixel that is below this average level is processed as a "zero". Several steps are required to convert a fingerprints unqiue features into a template, feature extraction. This is the basis for various vendors propriety algorithms (refs 5, 6, 7). For example, the fingerprint may be classified into whorls, loops or arches. Individual minutiae features such as ridges, forks and intersections can also be identified and their relative position captured and plotted by the application software. This data is then saved in a template for use in future comparisons or matches. Most software algorithms used to extract minutiae also compensate for minor deviations in the position of the finger on the optical scanning device. The process is usually one way, in that the template cannot be used to reconstruct the fingerprint.

Fingerprints can either be flat or rolled. A flat print captures an impression of the central area directly below the nail; a rolled print captures details of ridges on both sides of the fingertip. A slap captures multiple fingers (usually 4) simultaneously which are then segmented with segmentation software.

Fingerprint Acquisition Devices

Most common technologies include:

- Optical
- Capacitance
- Ultrasound
- Thermal imaging
- Inductive

Optical scanners are the most commonly used for AFIS applications (and enrolments for multiple fingers) because of their large area, high definition capture capability. Scanning fingerprints optically can be prone to error if the platen has a build up of dirt, grime, or oil—producing leftover prints from previous users (latent prints). Severe cases of latent prints can cause the superimposition of two sets of fingerprints and image degradation. Enrolments for multiple fingers are carried out on optical systems.

Capacitance sensors are frequently used for single finger applications (eg verification) due to their smaller area. The ridges and valleys of a fingertip create different charge distributions when in contact with a CMOS chip grid. This charge variation can be converted into an intensity value of a pixel via a number of DC or AC signal processing techniques.

Ultrasound scanning (ref 9) is designed to penetrate dirt and residue on the platens and has not been demonstrated in widespread use to date. An ultrasonic beam is scanned across the finger surface to measure the depth of the valleys directly from the reflected signal.

Thermal imaging (ref 10) uses a sensor manufactures from a pyroelectric material. Thermal imaging measures the temperature change due to the ridge-valley structure as the finger is swiped over the sensor. Since skin is a better thermal conductor than air, contact with the ridges causes a noticeable temperature drop on a heated surface. The technology is claimed to overcome wet and dry skin issues of optical scanners however, the resultant images tend to have a poorer dynamic range (not rich in grey values).

Fingerprint Compression and Template Algorithms

A typical finger has an image area of approximately ĺ xĺ and is recorded at 500 dpi with 8 bit greyscale. Compression techniques such as WSQ (wavelet scalar quantisation) are recommended over jpeg (ref NIST) and can offer up to 12.9 compression ratios. Templates are generated from the WSQ or JPEG image using proprietary software. Templates will be minutiae or pattern based and range in size range from 250 bytes to 1,000 bytes depending on which vendor's algorithm the system uses. Minutiae algorithms are used primarily for AFIS applications due to their higher processing speed and ability to cope with rotated fingers (a consequence of latent print capability). Pattern based algorithms are used primarily for physical and logical access applications where smaller cheaper sensors are used and therefore higher information density is required.

Fingerprint Advantages

Fingerprints are persistent: Fingerprints almost always remain the same throughout a person's lifetime except for accidental damage.

Fingerprints are unique: Every human has a unique set of fingerprints [reference]

Fingerprints are one of the most mature biometrics: Fingerprints have been widely studied and researched over the years and have been successfully used in most manual and automated methods.

The standards for interoperability of fingerprint systems are also the most mature biometric interchange standards. Also, despite the fact that 1 to 3% of people may find it difficult to reliable use a fingerprint system, fingerprints are the biometric with the largest population base in use worldwide.

Fingerprint Disadvantages

Dirt on the finger or injury can distort the image: An image of the fingerprint is captured by a scanner, enhanced, and converted into a template. During image enhancement the definition of the ridges is enhanced by reducing image noise. Sources of noise in reflective technologies arise because the reflected light is a function of skin characteristics. If the skin is too wet or too dry, the fingerprint impression can be saturated or faint and difficult to process. In addition noise may be caused by dirt, cuts, creases, scars or worn fingertips.

Contact system: In most current systems, the process of capturing the fingerprint biometric involves contact of the fingerprint pattern with an input device. Because of this, the actual pattern that is sensed may be elastically distorted during the acquisition of the pattern causing the possibility that impressions of the same finger may be quite different. There are some non-contact fingerprint sensors available that avoid the problems related to touch sensing, but these have yet to be proven on a large scale [ref digital descriptor].

Suppliers have propriety algorithms and matching hardware

Fingerprint Robustness and Vulnerabilities

As discussed, if a user leaves an oily latent image on the scanner, a false rejection may occur or someone with a fine brush and dry toner could "lift" fingerprints with adhesive tape. Latent prints can also be recovered by breathing onto the sensor window. Gelatin or carbon-doped silicon rubber can be used to mould finger templates from a wax imprint19. Some vendors include "liveness tests" to help against spoofing but it is likely to still be a developmental area

2.8.2 *Face*

Facial recognition is one of the oldest biometrics. Manual verification of a person against their photograph has been around for many years. It is also a non intrusive method for capturing a biometric.

Most systems to date have focussed on 2D images. Emerging techniques include 2.5D (multiple 2D images) and 3D (true 3D images).

Facial Image Acquisition Characteristics

Facial recognition technology identifies people by the sections of the face that are less susceptible to alteration—the upper outlines of the eye sockets, the areas around the cheekbones, the sides of the mouth and other prominent skull features.

Facial Image Acquisition Devices

Images can be recorded from static cameras or video cameras in the visible spectrum. Emerging technologies also make use of the NIR spectrum to mitigate for uncontrolled background illumination [ref A4Vision].

Facial Compression and Template Algorithms

Two primary methods of facial recognition system are used to create templates: (Other facial recognition technologies based on thermal patterns below the skin are not yet commercially available)11

- Local Feature Analysis
- Eigenface method.

LFA measures the relative distances between different landmarks on the face to create a facial biometric template, or faceprint. LFA uses many features from different regions of the face, and also incorporates the relative location of these features. The extracted (very small) features are building blocks, and both the type of blocks and their arrangement are used to identify/verify. Small shifts in a feature may cause a related shift in an adjacent feature and the technology can accommodate these changes in appearance or expression (such as smiling). LFA was patented by Visionics corp—now Identix Incorporated (ref 3). Since LFA does not provide a global representation of the face, it is prone to difficulties when the head is tilted away from the frontal pose by more than about 25 degrees horizontally or more than about 15 degrees vertically11.

The Eigenface method looks at the face as a whole and is patented at Massachusetts Institute of Technology (MIT). This method uses 2D global grayscale images that represent distinctive characteristics of a facial image.

The vast majority of faces can be reconstructed by combining features of approximately 100–125 eigenfaces. Upon enrollment, the subject's eigenface is mapped to a series of numbers (coefficients) that form the basis of the template.

Two other methods used in facial recognition systems are neural network and automatic face processing. Neural networks employ an algorithm to determine the similarity of the unique global features of live versus enrolled or reference faces, using as much of the facial image as possible. Automatic Face Processing (AFP) uses distances and distance ratios between easily acquired features such as eyes, end of nose, and corners of mouth. Though overall not as robust as eigenfaces, feature analysis, or neural network, AFP may be more effective in dimly lit, frontal image capture situations.

Facial recognition templates sizes are typically 83 to 1,000 bytes (ref 13).

Facial Recognition Advantages

Convenience and acceptance: Face identification is one of the most widely publicly accepted biometrics since it is not intrusive. It is relatively easy to perform face recognition and moderately convenient. Users tend to find it highly acceptable to be identified by their face since this is the most traditional way of identification.

Has potential for long distance recognition and covert identification from surveillance cameras

Has the potential to be applicable to existing image databases

Facial Recognition Disadvantages

Imaging conditions: The lighting of the face can have large effects on the appearance of the face in an image and therefore on the performance statistics.

Appearances naturally alter with age.

Although the passive nature of image capture rendered facial recognition easy to use, this is also the reason it is disliked; the face biometric is able to operate without the users cooperation, since CCTV camera need only capture a picture for the technology to generate a template. However, the technology is much more able to identify people who are motivated to cooperate with the system.

Facial Recognition Robustness and Vulnerability

Facial recognition systems tend to be less accurate than fingerprint systems [ref]. Impacts on performance and difficulties with acquiring facial images arise due to effects such as quick changes in facial expressions, unknown geometric location of the face upon presentation, imaging conditions such as lighting and compression artefacts. More on spoofing in here?

2.8.3 *Iris*

Iris recognition measures the iris pattern in the coloured part of the eye, although the iris colour has no role to play in the biometric. Iris patterns are formed randomly at birth and are the results of muscle tears as the eye forms [ref Iridian and Daugman]. As a result, iris patterns from left and right eyes of the same individual are different as are the patterns from identical twins (ref 18). Iris recognition has been developed primarily by Iridian (formerly IriScan) which holds over 200 patents.

Iris Acquisition Characteristics

Unique complex patterns of striations, freckles and fibrous structures in the human iris stabilise within one year of birth and remain constant throughout a lifetime. The iris can have more than 250 distinct features compared with 40 or 50 points of comparison in fingerprints (ref 14). John Daugman developed a set of mathematical formulae for iris recognition at Cambridge university in 1993 (ref 17). The patents for the algorithms are owned by Iridian Technologies and are the basis for current iris recognition systems and products. The concept patent expires within the next two years.

Iris Acquisition Devices

Systems require a camera to record the iris. Cameras can capture both eyes (binocular) or a single eye (monocular). The eye (or eyes) is initially located, the camera then zooms in and focuses on the eye itself, the iris is then located along with pupil boundary. Obstructed areas are located (eyelashes, eyelids) and the system then essentially breaks the image into circular grids and the each area analysed for unique patterns (using polar co-ordinate transforms). Feature vectors may be compared by Hamming distance and rotations.

Iris Compression and Template Algorithm

The majority of cameras generate the IrisCode algorithm in the camera. Raw images of the iris are difficult to obtain from Iridian approved "proof positive" iris cameras. IrisCode template sizes are 256 to 688 bytes.

Iris Advantages

Uniqueness—Iris development during gestation results in a uniqueness of the iris even between multi-birth children. These patterns are stable throughout life.

Non-invasive—No direct contact between the user and the camera.

Use of infrared band avoids uncomfortable visible illumination and improves contrast of iris, as well as seeing through some types of contact lens.

Facial images could also be captured at the same time as iris images are captured.

Iris Disadvantages

Image capture—Contact lens wearers or people with diseases such as glaucoma may find it difficult to pass an iris scan.

- Image capture—Correct illumination is required for good quality image capture.
- IP issues—fundamental patents owned by one company, Iridian.
- No large database of irises to assist in benchmarking systems.
- Extent and nature of exception cases needs study.

Iris Robustness and Vulnerability

Out of focus camera, mirrored sunglasses, contact lenses (patterned etc), glass eyes, medical conditions such as anirida and other such barriers to recognition may introduce system failures.

2.8.4 *Signature*

Dynamic signature verification is a behavioural biometric and is the automated method of examining an individuals signature. This technology examines characteristics such as speed, direction, pressure of writing, the time that the stylus is contact with a digitised platen, the total time to make the signature, and where the stylus us raised from and lowered onto the platen.

Signature recognition tends to be used more for document security than network log-ins.

2.8.5 *Voice*

Voice recognition is a reasonably common biometric technology [ref companies VeriVoice Motorola Ciphervox, Veritel corp voicecrypt2.01] for access control systems. Voice verification considers the quality, duration, pitch and loudness of the signal compared to previously enrolled characteristics. Speaker verification technologies can be divided into two major categories:

1. Text dependent—where the system associates a sentence or password, possibly different, to each user.
2. Text Independent—where the user is not requested to say the same sentence during each access.

Voice recognition can be affected by environmental factors such as background noise. Additionally, there is a concern that a voice could be recorded and played back for identification.

2.8.6 *Hand Geometry*

Hand or finger geometry utilises an automated measurement of many dimensions of the hand and fingers. Only spatial geometry is examined as the user places his or her hand on the sensor surface.

Digital camera captures two hand silhouettes. The hand needs to be aligned to posts, which may require some practice and good hand mobility. With a typical EER of 10-3, it is usually combined with a PIN or card.

2.8.7 *Vascular patterns*

Vascular pattern technology uses infrarered light to produce an image of the vein pattern in the face, back of hand, or on the wrist. Hand vein pattern readers measure the position of veins on the back of an individual's hand. Technical issues include the distance of veins from the surface of the person's skin, and the dilation or contraction of the vessels over time (due to aging or simply temperature changes).

2.8.8 *Retina*

Retinal scans measure the blood vessel patterns in the back of the eye. Users tend to perceive retinal scanning as intrusive and it has not gained popularity with end users. The device involves a light source that shines into the eye of the user who must be standing very still close to the device (within a few inches) as the compact sensor can see a significant part of the retina only from a very short distance. This makes the technqie slow and unergonomic. [one more sentence on how it works]. This biometric may have the potential to reveal more than just the identify of the user since patterns may change with certain medical conditions e.g. pregnancy, high blood pressure, AIDS.

2.8.9 *DNA*

This technique takes advantage of the different biological pattern of the DNA molecule between individuals. The molecular structure of DNA can be imagined as a zipper with each tooth represented by one of the letters A (Adeline), C (Cytosine), G (Guanine), T (Thymine) with opposite teeth forming one of two pairs, either A-T or G-C. The information in DNA is determined by the sequence of letters along the zipper and is the same for every cell in the body. The main concerns are the costs, ethical issues, practical issues and acceptability of the technology since DNA testing is neither real time nor unobtrusive.

2.8.10 *Gait*

The use of an individuals walking style or gait to determine identity. It is attractive because it requires no contact. Psychological studies support the view that gait can be modelled and is unique. It can be used to monitor people without their cooperation.

2.8.11 *Ear Recognition*

Ear recognition uses mainly two features:

— The shape of the ear: ear geometry—This technology utilises the fact that the shape and size of the ears are unique characteristics of an individual.

— The canal of the ear which returns a specific echo: otoacoustic emissions.

While ear geometry has been used by police to identify criminals, otoacoustic emissions are currently the subject of academic research. Tests carried out by University researchers indicate that if clicks are broadcast into the human ear, a healthy ear will send a response back15. These are called otoacoustic emissions.

2.8.12 *Keystroke*

Keystroke dynamics is an automated technique of examining a users fluctuating typing dynamics. People move their fingers around the keyboard in precise, yet irregular, timing patterns during log ins without even realising it. Characteristics such as speed, pressure, total time to type a password and the time between hitting different keys are measured. The algorithms are still being developed to improve robustness and distinctiveness. NetNanny Software Inc bases a keystroke biometric on patented algorithms originally developed at Stanford University and measures the timings between keystrokes. There are issues around personal privacy in the commercial use of keystroke dynamics—such as applications to monitor hourly progress of employees.

2.8.13 *Other*

— Body odor (This technique is under development and relies on an individual's distinctive smell from chemicals known as rolatiles)

— Lip motion

— Skin Reflectance

— Thermogram

2.9 *Market Structure*

The supply chain for biometrics comprises

— Biometric hardware providers

— Biometric software providers

— Biometric hardware and software providers

In terms of individual biometrics fingerprint and face dominate the market in terms of supplier numbers. There are 100's of fingerprint companies although only 4–5 AFIS suppliers. The rest of the fingerprint companies are primarily logical and physical access companies of which about 10 are well known names.

These 10 also offer other biometrics such as face. In terms of large area optical capture devices there are up to 10 companies that offer solutions. Capacitance "flat" capture chips are offered by approximately 5 suppliers, some of which are fables. There are 100's of companies that then package these chips in a variety of formats: USB readers, PCMCIA card, standalone, combined with card etc. Some of the larger AFIS suppliers are able to be the prime contractor for medium scale biometric projects.

The face market has fewer companies with 10's offering 2D solutions and approximately 10 offering 3D solutions.

The iris market is effectively controlled by Iridian with approximately 4–5 companies offering Iridian approved ("proof positive") cameras. Another company Iritech is developing its own iris solutions. Other iris companies offer access control and border control solutions.

The other biometrics are generally represented by a small number (< 10) of companies with the possible exception of finger and voice.

3. Biometric Trials

The UKPS Biometric Enrolment trial was governed by a Project Board with representatives from the contractors, Atos Origin, UKPS and the Identity Cards Programme and also Dr Tony Mansfield from National Physical Laboratory (NPL) who advised on the experimental design. The trial final report was reviewed by those close to the trial within the Identity Cards Programme and also by Professor Paul Wiles, the Home Office's chief scientist and by Dr Tony Mansfield of NPL.

Dr Mansfield was co-author of the earlier feasibility study on the use of biometrics in an entitlement card scheme, referred to as the "NPL feasibility study. There was no formal project structure to oversee its production.

The following note shows the comments on trial report from Dr Tony Mansfield. These were in general very specific comments on the text of the report which were incorporated into the final version of the report.

UKPS Biometrics Enrolment Trial Comments on Final Report (version of 25.02.05)

Dr Tony Mansfield, National Physical Laboratory, 10 March 2005

Overall Comments

How does the trial "help inform Government plans to introduce biometrics"

- Some of the report might be better focussed if the management summary provided a list of questions that the trial was trying to answer, and then the report provided detail on what the trial indicated in response to these questions. (I am sure that many of these questions are listed in documents at the commencement of the contract.)
- I feel the analysis does not quite go far enough to answer many of the questions that need to be answered (even though the trial may provide the required data).

Recommendations

- I find the recommendations rather bland—many would have been obvious prior to the trial. There are more substantial recommendations to be made:
  - I believe the trial has provided data to indicate how long biometric enrolment ought to take—taking account of both public acceptability, and the capabilities of the technology.
  - There could be clearer recommendations about the adequacy of current technology. All the systems need improvement, especially in the user and operator interfaces.
  - The environment recommendations ought to note that the current enrolment pod did not sufficiently control the environment.
  - The report (and previous versions) made a number of observations where causes of problems merited further investigation. These should be listed.
  - A categorisation of types of exception cases, and their extent, would lead to a recommendation that future tests include such cases to check that necessary system improvements have been made.
  - I would have expected a number of recommendations in regard of any future trial—surely many lessons were learned by the problems encountered during the trial setup!
- Recommendations that are made could also have more substance.
  - Eg the trial shows that allowing longer enrolment times with the existing system will not achieve the required improvement in enrolment success rate, even if publicly-acceptable enrolment times are exceeded. However the recommendation for a secondary enrolment system with different interfaces is made without this justification.

Report structure

— Section 1 is somewhat long for an executive summary. Could this section commence with a shorter overview (of a page or so) that provides highlights of the main findings.

— Some key findings, such as identifying demographic groups with greater concerns and greater difficulties in using the systems, are missing from the summary.

— Annexes should not to contain key findings or recommendations beyond those in the body of the report. Could Annex C2 be moved to the main part of the report. Alternatively there could be sections listing all recommendations and all key findings together.

Additional sections

— The summary should include some details of the affect of demographics on performance and attitudes.

— I could not see a section discussing the views of the enrolment staff as to the ease of use or problems with the systems used (as per a previous suggestion).

— Add an annex providing a copy of the questionnaire.

— Add an annex explaining acronyms.

Wording

— The report could be more carefully worded in several places.To take one case, the majority of trial participants were unconcerned about booth privacy—what is written is "booth privacy is not an issue across all groups"—this seems rather dismissive of the views of the minority. Factors which affect only a few individuals may still be an issue that has to be addressed in deploying biometrics. Also, it is unclear whether "all groups" refers here to the Quota, Disabled, and Opportunistic groups or to all all demographic groups. There is similar wording in many places in the report.

Section on Standards

— The review of international standards in Annex C3 omits the work of the international standards committee SC37 (apart from referring to the US shadow committee INCITS M1—and it would have been more appropriate to refer to the equivalent UK committee BSI/IST44). This annex does not add anything to the report, and does not relate to any of the trial findings—I suggest this is removing this section from the released version of the report.

DETAILED COMMENTS

p10—§1.1.1—para 1, sentence 1

I thought ATOS designed the trial (as stated in 1.1.2).

Change "*designed by UKPS*" to "*commissioned by UKPS*"

p10—§1.1.1—para 3 "specific objectives",

What is listed is the work to be done. I would have thought the specific objectives would have been the list of questions to be answered by the trial.

p10—§1.1.1—para 2, last sentence

Trial results about attitudes are independent of software and hardware used.

Change "*All the trial results*" to "*The trial results*".

p13—§1.1.4—Recording the iris biometric—1st paragraph

As stated, the right iris would be enrolled only once the left iris is successfully enrolled. This does not accord with my recollection of enrolment.

p13—§1.1.4—Recording the iris biometric, and recording the fingerprint biometric, last lines.

How many times was a duplicate enrolment was detected should be stated.

p14—§1.1.4—Recording electronic signature, para 2

This paragraph refers to all the previous steps, not just recording signature.

Remove the indentation.

p15—§1.2.2—Booth privacy

Awkward wording and poor grammar. Suggest changing to:
"*Within the locations and environments used in the trial. few participants had concerns over booth privacy. 94% of the quota group, 89% of the opportunistic group, and 87% of the disabled group were not at all or not very concerned about privacy in the booth during the enrolment process*".

Similar changes are required elsewhere:
Level of intrusion
Ease and speed of verification
and other places too (search for "not an issue", "not a concern")

p15—§1.2.2—Time taken

Awkward wording.
"*[Enrolment] . . . was some 8 minutes on average. The figures were not equal across the three biometrics . . .* ". This implies that 8 minutes is the average enrolment time for a single biometric! I suggest changing to:
"The total time needed to enrol face, iris and fingerprint biometrics was about 8 minutes on averaged. For each of the quota, disabled and opportunistic groups, the time required for biometric enrolment was generally as expected, or faster than expected. The iris biometric had the greatest number(18%-21%) of participants who found the experience slower than expected.

p15—§1.2.2—Time taken, line 1

Delete "*experienced*"

p21—§1.3.2—Facial enrolment success, last line.

First attempt enrolment success rate is a rather esoteric performance metric, which is not as operationally relevant as the overall enrolment success rate, or the time required. I suggest it is inappropriate to introduce this metric in the management summary.

p21—§1.3.2—Iris enrolment success, last sentence

The analysis mentioned here is not described in the body of the report. My inclination would be to delete this sentence, or replace it with *"enrolment operators felt that the lack of feedback from the iris camera made it difficult for them to establish reasons for enrolment failure and to advise corrective action."*

p23—§1.3.3—Iris verification success, 2nd paragraph

As it is not clear whether this observation (removing glasses improves iris verification success or whether it is taking a 2nd attempt that improves iris verification success) is significant, it should be omitted from the summary.

p23—§1.3.3—Fingerprint verification success, 2nd sentence

Poor grammar.

"One of the factors causing a failure at verification was that the single-finger sensor used for verification occasionally did not record sufficient detail from the fingerprint.

p23—§1.4.1—Main recommendation

I don't see this as the most important recommendation from the trial. Perhaps this should be titled "*Back-up solution/secondary capture devices"*

p25—§1.5

Surely there should be a conclusion on the adequacy of the technologies used.

p25—§1.5—last sentence

Change to *"Room or pod design should be thoroughly reviewed . . ."*

p29—§2.2

I think that the equipment and technology used is relevant enough to include in the body of the report. Perhaps summarise in the form of a table, and refer to the Annex for full details.

p78—§5.2 paragraph 1, last 2 lines.

The opportunistic sample was not a randomly picked sample of the general public as stated here. (By design, the quota sample should be a good indicator for a random sample!)

p297—Time taken vs participant response graphs

The way these graphs are plotted is hiding any information that may be gleaned from such graphs. The tails (long enrolment times) appear as zero—the height of the curves are not comparable, as results are not normalised against the number of responses in each category—and the bin sizes for enrolment times are too large, so we cannot really see any difference in the shape and skew of the curves.

p314—§E3.1

9^8 (Looks like 9 to power 8) Move the footnote mark (8) from "*9"* to "*failed*".

Next Page: Extract from a submission to Andy Burnham on the publication of the UKPS trial final report.

Note that paragraph 5 in this submission refers to the decision to delay publication of the final report. The UKPS had planned to publish the Biometric Enrolment Trial report on 28 April 2005 alongside other Home Office research scheduled for that day. However, that date fell in the week prior to the General Election. In line with the General Election guidance (published by the Cabinet Office); UKPS sought advice as to whether publication in April would be acceptable. The advice received from the Cabinet Office was that publication should be delayed until after the election.

From:	Rob Bowley	cc:	Home Secretary
			Tony McNulty
	Director Identity Projects		John Gieve
	UK Passport Service		Helen Edwards
	8th Floor		Paul WilesKatherine Courtney
			Stephen Harrison
	Tel: 020 7901 XXXX		Robert Raine
			Henry BloomfieldPaul Wylie
To:	Andy Burnham		Christine Nickles
			Vivienne Parsons
			Peter Wilson
			Special Advisers
Date:	12 May 2005		

UKPS BIOMETRIC ENROLMENT TRIAL—REPORT

ISSUE

1. When to publish the UKPS Biometric Enrolment Trial Report

TIMING

2. Immediate

RECOMMENDATION

3. The report of the trial to be published on 26th May 2005. Research reports are normally published on the last Thursday of the month unless there are good reasons for publishing on another date.

SUMMARY

4. Contractors (Atos Origin) completed the report of the Biometrics Trial and submitted it to UKPS for quality assurance on 25 February. We have previously stated in a PQ to Mark Oaten that the report would be published by the end of March. That date fell because of the work needed to ensure that the findings were statistically robust and presented to best effect. There was a particular issue with the findings for people with disabilities for whom the success in enrolling in the scheme and the results in the attitude survey were relatively less favourable than for the rest of the population MORI and Disability Matters were consulted and their views incorporated.

5. The report was not taken to a conclusion for publication in April because of the General Election.

6. The quality assurance of the final report is now complete and in line with the Home Secretary's preference for research to be published on the last Thursday in the month, The report should be scheduled published on May 26 2005. Any further delay will cause adverse comment.

7. A handling submission will follow once the date for publication has been agreed.

SUPPORTING INFORMATION

8. The UKPS biometric trial began on April 14th last year and was closed on 24th December 2004 after over 10,000 enrolments had been completed.

9. Its objectives were to:

- test the use of biometrics through a simulation of the passport process
- include exception cases, e.g. people who may have difficulties in enrolment
- measure the process times
- assess customer perceptions and reactions
- assess practical aspects of incorporation of biometrics into a biometric database
- test fingerprint and iris biometrics for one-to-many identification and facial recognition for one-to-one verification

Although the trial was run by UKPS, we have been explicit that it is also preparatory to the introduction of ID Cards, and the bulk of its cost has been met from Home Office budgets.

10. It was not a technology trial i.e. we did not try a range of equipment and compare performance of each unit nor the interoperability of various systems.

11. The trial engaged with 10,000 volunteers from across the UK providing a cross section of the UK population. The participants fell into three broad categories:

— Quota sample of 2,000 *(a representative cross-section of the UK population)*

— Opportunistic sample of 7,250 *(people who self-selected their participation)*

12. Disabled sample of 750 which was collected against the original requirement of 1,000. Statistically this reduction in sample size did not have any material effect on the results. Disability Matters, a leading disabled community interst group, have contributed to the quality assurance of the report. They were also engaged by Atos Origin, the contractor, to help in the recruitment of the sample of disabled people.

13. To achieve trial objectives four fixed sites and one mobile unit were employed during the trial. The four fixed sites were located at:

UK Passport Office London

Newcastle Registrars Office

Leicester Post Office

DVLA Local Office Glasgow

14. The route of the Mobile Unit was chosen to allow participants from the disabled community as well as able-bodied to experience the process. Venues included Highbury College Portsmouth, RNIB Redhill, National Association for Epilepsy Chalfont St. Peters, Enham Alamein Andover and the St. Loyes Foundation Exeter.

15. Overall, the trial indicated a positive participant response to both the process and concepts of biometrics. The majority of participants were in favour of the adoption of biometrics as a means of identification, believing that it would help prevent identity theft and prevent illegal immigration. The majority of participants in all sample groups also successfully enrolled on all three biometrics, with success rates of 89% for quota participants, 90% for opportunistic participants and 61% for disabled sample participants. 100% of quota and opportunistic sample participants and over 99% of disabled sample participants were able to enrol successfully at least one biometric i.e. face, fingers or iris.

16. The trial was particularly designed to find out which groups of the UK population may have difficulties with biometric enrolment. Although the trial was not a trial of the technology or equipment and all results need to be seen in the context of the particular hardware and software configurations used. It is clear that some equipment used in the trial gave better results than others. The equipment was however able to test processes, customer reactions and perceptions as intended.

17. Across the trial results the sectors experiencing most problems with biometrics enrolment in general were the elderly, disabled and participants drawn from black and other minority ethnic (BME) groups.

Some specific issues identified are:

Facial biometrics:

18. 99.74% of participants in each sample group successfully enrolled a facial biometric. However, the failure rate for the disabled sample group was significantly higher than that for the quota and opportunistic groups. White participants had a higher first attempt facial enrolment success rate than black participants while facial verification success rate was higher for participants aged under 60 than it was for those aged over 60. The exact reasons for these inconsistencies are not currently evident from the report of the trial and require further investigation, which we have requested.

19. Maintaining the correct position for facial biometric enrolment was a problem for some disabled sample participants with a physical impairment or with learning disabilities and also some elderly persons.

Iris biometrics:

20. 88.36% of participants successfully enrolled their Irises. The disabled group achieved significantly lower results at 61%. It appears that this was mainly due to positioning and behavioural issues. i.e. where the participant could not place themselves in the correct relationship to the camera or could not follow the camera and operator instructions. Some participants also volunteered existing medical conditions that apparently adversely affected their ability to enrol.

21. Iris enrolment success, and success at the first attempt also varied according to the participant's ethnic group and age. Asian and white participants had higher success rates than black participants. Younger participants had higher success rates than older participants. Additional work is required to ascertain the exact reasons behind these findings and to test their statistical validity.

Finger biometrics:

22. 99.03% overall successfully provided finger scans. This fingerprint enrolment success was lower for black participants than other groups (97.72% of the sample tested). Participants with a learning disability and participants with a physical impairment had lower overall finger success and first time success than other participants in the disabled sample and those from the quota and opportunistic participants.

23. The 55 + yr age group found it more difficult to position themselves for the finger biometric than the 18–34yr and 35–54yr age groups. Some disabled customers could not physically position their fingers correctly and/or position their wheelchairs close enough to the machine.

General:

24. A small percentage (0.62%) of disabled sample participants failed to enrol on any of the biometrics. In these cases biometrics could have been gathered but the process was halted at the operators discretion for the comfort of the individual.

25. Over 80% of participants supported the use of Biometrics and over 90% found the process not to be intrusive.

26. The sectors most likely to believe biometrics are an infringement on their civil liberties are 18-34yrs, the C2DE social group and the BME sectors.

Further Work Recommended from the Trial

27. Additional work should be undertaken to further investigate the findings surrounding the enrolment of the BME sector and the elderly. Also that specific work addressing the needs of the disabled community should be carried out in co-operation with appropriate specialist organisations.

28. UKPS and the ID Cards Programme are currently drawing up plans to follow up these recommendations with the emphasis on comparative equipment trials, large database trials and later (possibly tied in to the UKPS Authentication by Interview project) and larger scale public trials.

4. Advice from Biometric Experts

The Biometrics Experts Group is a group of Home Office and external experts which meets approximately once a month. Its role is to actively contribute to the biometrics requirements of the programme, in contrast with the Biometrics Assurance Group, which provides assurance.

Minutes are taken of meetings but contain details of the proposed testing and evaluation of vendors' biometric solutions and their release may compromise the procurement process.

When it met on 26/27 January the attendees were:

Tony Mansfield	NPL
Jim Wayman	San Jose State University
Philip Statham	CESG
Chris White	CESG
Bill Perry	UKPS
Marek Rejman-Green	Home Office (27th only)
Kok Fu Pang	Home Office
Zoe Nicholson	Home Office IDCP (26th pm only)
Duncan Westland	Home Office IDCP
Peter Durant	Home Office IDCP

5. The Biometrics Assurance Group

You asked for membership of the Biometrics Assurance Group, the meetings it has held and for copies of any reports reproduced.

Current membership of the group is reproduced below. In addition to the Chair who is Professor Sir David King the Government's Chief Scientific Adviser and head of the Office of Science and Technology there are due to be 10 members, of these the 7 below have taken up their role. The Biometrics Assurance Group met on the 24 November 2005 and again on the 20 February 2006. It is next due to meet on the 15 May with further meetings in July, September and December of this year.

The Biometric Assurance Group is to issue regular reports, possibly to a June/December timetable.

It is worth noting some of these details may change. At its last meeting the Biometrics Assurance Group elected to form a number of sub groups each with a tighter remit which may require additional resource. This may lead to an increase in membership and group activity.

Biometric Assurance Group Members

Chair	Sir David King	UK Government Chief Scientific Adviser
Member	Angela Sasse	University College London
Member	Dick Mabbott	APACS
Member	John Daugman	University of Cambridge
Member	Mike Fairhurst	University of Kent
Member	Peter Hawkes	British Technology Group
Member	Peter Waggett	IBM
Member	Valorie Valencia	Authenti-Corp

The functions of the Biometric Assurance Group are: Ensuring Programme's requirements for biometrics, biometrics testing and biometrics procurement are adequately specified.

— Evaluating the biometrics elements of proposed solutions offered by suppliers and integrators.

— There may be some work on reviewing and interpreting the outcomes of testing.

— Reviewing the advice the Programme receives from its experts and offering advice in those areas that are unclear.

— Reporting to the director, SRO and the Programme board.

— Identifying emerging issues

6. Advice on IT

External advice is provided by:

— Contractors

— Other parts of government, eg other departments, CSIA (Central Sponsor for Information Assurance), CESG (Communications Electronic Security Group)

— Market sounding exercises

We have adopted for reference and evaluation purposes a modular architectural design approach based on a "Service-Oriented Architecture" where module requirements can be met wherever possible by customised versions of systems commonly found in the marketplace and where communications between modules takes the form of simple, highly-structured service-oriented messages. These reference solutions are for the purposes of developing requirements and evaluating proposals. The eventual system design will be done by the suppliers, chosen through open competition.

This modularisation is intended to simplify, and hence help de-risk, IT system delivery, and allow easier substitution of any modules that fail to meet our capability, performance and resilience requirements without a complete re-engineering of the solution. It should also permit the simpler "debugging" of problems and attempted security violations since information flows between systems will be visible and auditable.

For biometric matching systems, we have conducted detailed market soundings about the types of systems typically used by biometric suppliers for this purpose (eg, general purpose blades, conventional rack-mount servers with custom ASIC/FPGA-based PCI cards) and performed a space-and-power requirements analysis within the limits of the information provided by suppliers.

We are currently considering how to specify—and validate delivery of—IT systems, both individually and operating in unison, that are tolerant of unpredictable load conditions (including major overloads) ensuring service continuity is maintained at all times e.g., by slowing down rather than crashing. We also are examining the most appropriate replicated system configuration across multiple sites to ensure minimal service disruption in the event of a "disaster".

Assurance on IT is provided by the programme team, by our independent assurance panel and by external reviews—eg by the Home Office Science and Technology Reference Group.

7. PA Consulting

Note on role, involvement and responsibilities of PA Consulting Ltd work for Home Office Identity Cards Programme.

It was identified in 2004 that the Home Office did not have ready access to certain skill sets and resources necessary for implementation of a large and complex project such as Identity Cards. In addition it was seen that it would be beneficial to have a mixture of public and private sector expertise in the programme.

To address this need a client-side "Development Partner" was procured to bring in support to determine the best way of designing and implementing the proposed scheme. In line with normal practice on procurement of consulting services of this type, approaches were made to a number of companies who have framework arrangements with the Office of Government Commerce to provide management and business consultancy to Government departments—details of the framework at www.s-cat.gov.uk

The contract was let as a result of evaluation of proposals received, which were assessed on a Value for Money basis. This resulted in a contract being awarded to PA Consulting Ltd for the development and procurement phases of the Programme.

PA provides expertise and resource to the programme covering a number of different skills. This is in the form of embedded resource—PA work as part of the programme team along side civil servants and seconded staff to deliver programme outputs. PA support the design, feasibility testing, security accreditation, business case and procurement elements of the proposed scheme. The specialist skills include project and programme management, procurement, smart cards and biometrics, business process design, financial modelling and business case development.

APPENDIX 3

Memorandum from the UK Computing Research Committee

SUMMARY

UKCRC is an independent, expert body whose members are leading researchers in computing. We have experience of offering scientific advice to Government in an area that is central to the Science and Technology Committee's first case-study: the technologies supporting the Government's proposals for identity cards.

This paper summarises the occasions on which we have offered scientific advice and any follow-up by Government departments or related bodies. We conclude that Government has made no real attempt to base computing policy on scientific evidence.

INTRODUCTION

1. This evidence is submitted by the UK Computing Research Committee (UKCRC), an Expert Panel of the British Computer Society (BCS), the Institution of Electrical Engineers (IEE) and the Council of Professors and Heads of Computing (CPHC). The UK ranks first or second in the world in many areas of computing research. UKCRC was formed in November 2000 as a policy committee for computing research in the UK; its members are leading computing researchers from UK academia and industry; within our membership we have considerable experience of applying scientific methods to the problems of building industrial-scale computer-based systems.

2. Our area of expertise addresses a central element of the first of your chosen case-studies: the technologies supporting the Government's proposals for identity cards.

3. The UK computing research community is committed to addressing areas of national importance, as well as those of scientific promise. We devote significant efforts to engagement with industry and with users of our technology. As a consequence, UKCRC has substantial recent experience of offering scientific evidence to inform Government policy in these technologies. As an independent expert panel of the two relevant Professional Institutions, we are able to provide scientifically sound advice that is visibly free from any commercial bias.

4. UKCRC members are involved in several departmental advisory committees, including the Council for Science and Technology (CST), the Scottish Science Advisory Committee (SSAC), and the Defence Science Advisory Committee (DSAC).

5. UKCRC members have acted as expert witnesses in major litigation over failed computing projects. We welcome any opportunity to provide assistance that would reduce the risk of such failures in the future.

6. We believe that greater use of modern computing science would substantially reduce the risk of overrun or failure of the computer-based projects that are an essential part of the Government's strategy for e-Government and the modernisation of public services, potentially saving hundreds of millions of pounds each year and improving service delivery and security. The relevant computing science includes mathematically rigorous approaches to specifying and validating systems, security and dependability technologies, statistically-based methods of system evaluation, and science-based engineering methods. We have suggested that Government could take active steps to encourage the software industry to develop, document and share best practice, working through the professional bodies, and perhaps extending as far as accreditation.

7. We have evidence that science-based development methods are practical and cost-effective. They are used by some organisations to great effect: Microsoft, for example, uses rigorous mathematical approaches to designing and specifying systems (for example, the program analysis tool PREfix, which is widely used by developers within the Company for automatic "program review" before testing or delivery, and the Windows static device driver verifier tool), and some statistical techniques for systems evaluation. The Motor industry and the aircraft industry are also increasingly using mathematically formal development methods cost-effectively.

What advice have we given?

8. We have sought the opportunity to present this evidence to policy makers. We believe that the case history of our recent engagement with policy will illuminate the extent to which ministers and scientific advisors consider scientific evidence in formulating policy in our area of expertise.

9. Overall, we have been disappointed with the extent to which scientific evidence has been sought or used in our area of expertise. This may be due to the difficulty of understanding the issues associated with building non-physical systems of great complexity, but we believe that computing science is in general no more complex that many other areas of science.

10. In November 2002, UKCRC sought and achieved a meeting with Science Minister, Lord Sainsbury. We explained the great opportunities open to the UK to benefit from exploiting the UK's leading position in computing science research. Lord Sainsbury said that he was very interested and asked us to contact the Information Age Partnership (David Jordan), the Office of Government Commerce (David Hughes) and EPSRC (John O'Reilly). He also asked for a briefing paper on educational technology, which we provided. There was no other follow-up by his Department.

11. UKCRC met David Jordan in February 2003 and offered to contribute expertise to the Information Age Partnership. We were told that it would be inappropriate for UKCRC to become a member of the IAP but that we could provide very valuable input to their work. To date we have not been asked for any assistance.

12. UKCRC met David Hughes (OGC) and John O'Reilly (EPSRC) in April 2003, where we again offered expertise to help transfer computing science into industrial use, to benefit the public sector and industry. The meeting went well, but David Hughes said he had to wait for the replacement of Peter Gershon as OGC Director before organising a follow-up meeting. Despite reminders, and constructive criticism of the OGC's procurement guidelines for computer-based business change projects, no such follow-up has occurred.

13. John O'Reilly said that it would be inappropriate for EPSRC to have further meetings with UKCRC alone, but that he would welcome UKCRC's involvement in his meeting with the BCS, IEE and CPHC.

14. In April 2003, the Royal Academy of Engineering and the British Computer Society (BCS) published a report: *The Challenges of Complex IT Projects.* Several UKCRC members had contributed to the report, which called for the introduction of "Systems Architects" to support the use of better science and engineering in the development of complex IT projects. (Systems Architects would be people with advanced skills in adopting rigorous approaches to software development and project evaluation). Despite repeated efforts by the BCS, the Royal Academy, the Institution of Electrical Engineers and UKCRC, no Government Department has adopted this recommendation or (so far as we are aware) asked for a meeting to discuss it further.

15. In 2004, UKCRC responded to the Home Affairs Select Committee Inquiry into the Government's proposals for ID Cards and a National Identity Register. We gave written and oral evidence, arguing once more that the use of better computer science could reduce the high risk of overruns or failure of this project. We have followed this up with a meeting with the Home Office official managing the ID card project, and with two meetings organised by the Law Society attended by a Home Office Minister and officials. We have not been asked to clarify or expand on the ideas we presented at these meetings.

16. Also in 2004, UKCRC assisted the National Audit Office's review of the National Programme for IT in the Health Service (NPfIT—now *Connecting for Health*). We discussed the system issues and risks, and drafted a check-list of simple questions which was also sent to the *Connecting for Health* team. They have not requested a meeting with UKCRC.

17. In October 2004, UKCRC responded to a call for evidence on Civil Service effectiveness by the Public Affairs Select Committee. We gave written evidence on the difficulty we were having in influencing the civil service to base their computer systems procurement policy on the best computing science and software engineering.

18. UKCRC members have been involved in the advisory panels for several Foresight Directorate projects. This has given us the opportunity to raise with Sir David King (Chief Scientific Adviser) the difficulty of getting Government Departments to engage with first class computing science and engineering. Sir David King asked for a briefing paper and made an oral commitment to "make something happen". The

briefing paper was sent to Sir David on 10 May 2005. On 8 August, after reminders, his office replied that it had been forwarded to the Head of e-Government, Ian Watmore, who would set up a meeting. Despite further reminders, no meeting has been set up.

19. Copies of the briefing papers, reports and presentations referred to above can be provided to the committee on request.

20. This (incomplete) chronology provides the background to our answers to your specific questions, below.

Answers to Specific Questions

Sources and handling of advice

21. What impact are departmental Chief Scientific Advisers having on the policy making process? In our experience, none.

22. What is the role of the Government Chief Scientific Adviser in the policy making process and what impact has he made to date? The Chief Scientific Adviser seems unable to influence the policy making process in our area.

23. Are existing advisory bodies being used in a satisfactory manner? We see little evidence that they are effective in stimulating the take-up of relevant computing science.

24. Are Government departments establishing the right balance between maintaining an in-house scientific capability and accessing external advice? Our interpretation of the recently published Government IT Strategy is that the Chief Information Officer has recognized that the Government needs to rebuild and nurture departmental expertise in Computing. UKCRC will respond to the current consultation on this IT Strategy. To date, external advice on computing policy has been sought primarily from Intellect, the trade body that represents the UK IT industry, and whose members have been involved in almost all of the public sector IT projects that have overrun or failed. The voice of industry is important, of course, but it cannot be expected to be free of commercial bias.

Relationship between scientific advice and policy development

25. What mechanisms are in place to ensure that policies are based on available evidence? In this area, none that we have been able to discover.

26. Are departments engaging effectively in horizon scanning activities and how are these influencing policy? The Foresight projects in CyberTrust and Intelligent Infrastructures are excellent examples of horizon scanning. It is too early to know how much their output will influence policy. UKCRC has been calling for urgent action, based on the best science and engineering that is currently available for exploitation (most of which originated in the 1980s and 1990s). There is little point in horizon scanning unless you are already using the best science currently available!

27. Is Government managing scientific advice on cross-departmental issues effectively? Our experiences with the Chief Scientific Adviser and with the NAO suggest that cross-departmental issues are a severe barrier to effective action.

Treatment of risk

28. Is risk being analysed in a consistent and appropriate manner across Government? Poor risk analysis and risk management is repeatedly identified as a significant factor in the failure of public sector IT-enabled business change projects.

29. Has the precautionary principle been adequately defined and is it being applied consistently and appropriately across Government? We understand the precautionary principle to be the principle that where a scientific advance or new technology poses unquantifiable risks to health or the environment, it should not be licensed for use until the risks are sufficiently well understood. The use of computing science does not present such risks; indeed, a major benefit of greater use of rigorous, science-based methods would be that the risks of projects overrunning or failing would become smaller and easier to manage.

30. How does the media treatment of risk issues impact on the Government approach? We do not have relevant experience to answer this.

Transparency, communication and public engagement

31. Is there sufficient transparency in the process by which scientific advice is incorporated into policy development? No. It is unclear how science influences Government computing policy, if it does at all.

32. Is publicly-funded research informing policy development being published? Yes, a great deal of excellent research that should inform policy development is published every year by the academic community. For example, the EPSRC Interdisciplinary Research Collaboration on Dependability has

published many papers and two or three books on approaches to assuring dependability in complex, socio-technical systems. Some of this work has informed policy—for example, MoD has incorporated some of the work in revisions to Defence Standards, and National Air Traffic Services Ltd are paying serious attention to some counterintuitive results on the negative impact of advisory systems on the performance of human experts—but this results from specific action by individual researchers rather than from any Government policy to track and utilise research.

33. Is scientific advice being communicated effectively to the public? UKCRC, the BCS, the IEE, the RAEng, EPSRC and many others do our best in the computing area. The media's appetite for scientific advice is sporadic and tends to focus on *post-hoc* discussions about problems (such as difficulties with the Inland Revenue systems or the Child Support Agency) rather than on policy formation.

Evaluation and follow-up

34. Are peer review and other quality assurance mechanisms working well? Our main experience is with EPSRC, where peer review works well in general, but it is often difficult to get peer support for work which would provide the sort of evidence, for example metrics from large-scale projects, on which policy ought to be based.

35. What steps are taken to re-evaluate the evidence base after the implementation of policy? We look forward to having some evidence-based policy to evaluate!

Conclusion

36. Our experience leads us to conclude that the Government has made no real attempt to base computing policy on scientific evidence, possibly because so many departments would be affected by changes in computing policy, and because there is a powerful industry group that has shown little interest in greater adoption of science-based engineering methods (other than in highly safety-critical or security-critical applications). In our opinion, such considerations should not be allowed to become a barrier to proper consideration of the evidence, nor to carrying out limited trials. The potential benefits are very great indeed.

37. UKCRC would welcome the opportunity to assist the Committee by clarifying or expanding on any of the points above.

January 2006

APPENDIX 4

Memorandum from the Institute of Electrical Engineers (IEE)

The IEE responds to around 30 formal consultations each year, as well as maintaining regular contacts with a number of government departments. Much of this work is of a technical nature (see Annex 1), and we form our views based on advice from our panels of expert Members and Fellows. In addition, our Members and Fellow sit on a variety of government advisory panels and committees (for example the Council for Science and Technology), as either individuals or representing the Institution, and are also heavily involved with activities such as the Research Assessment Exercise (RAE). The IEE is therefore pleased to submit evidence to this House of Commons Science & Technology Select Committee Inquiry.

It is rarely possible for us to establish a direct link between evidence offered to government and its policy decisions. This position does not seem to be unique to us, and in our experience it is generally felt there is very little in terms of published analysis or feedback. The exception is typically where a summary of consultation responses is produced, yet this is still unlikely to explain what evidence was, or was not, used in the decision making process.

In contrast to this, there are some notable successes. Foresight[3] is widely perceived as a valuable exercise, which considers future issues, and enjoys strong participation and a two way exchange, with the wider science and technology community. Yet Foresight is perhaps in a unique position, with different time scales, and a focus on the issues of tomorrow, not today.

Scientific evidence is extremely important in policy making because not everyone involved is going to have a natural understanding of the issues. Scientific and technical evidence needs rigorous analysis and should be subject to peer review, although time pressures must be taken into account. Even when timeliness is critical, the use of existing panels/committee of experts, or looking to professional institutions or other bodies could be a quick route to getting the necessary analysis to be done—yet in our experience assistance is seldom requested.

[3] http://www.foresight.gov.uk/

Government already has guidelines produced by the Office of Science and Technology. These guidelines are extremely comprehensive, and provide the right framework for Government. The one weakness, as we highlighted in August 2005 when we were consulted, is evaluation and monitoring.

The Technologies Supporting the Government's Proposals for Identity Cards

The Home Office carried out a major consultation over an extended period, and received input from an extremely wide group of stakeholders including the IEE. Our input was gathered from—as it always is—a broad range of members, many of whom are leading experts in the various sciences and technologies. We offered this advice impartially and raised a number of important issues, including those concerning the technical implementation of the scheme, such as the technical aspects of biometrics, and the more general problems encountered time and again with complex IT systems.

The Home Office published a summary of the responses in October 2004. Whilst this appears to be very comprehensive, it is simply a summary. It did not detail what arguments were accepted, or how the scheme as taken forward will address the issues. This lack of open and informed debate continues.

There may be some value if future summary documents included information on the response to certain evidence, what was accepted/rejected, or how proposals have been amended. This type of feedback would be useful both for those outside Government to understand the decision, and the process leading to that decision, and might also to improve the quality of future inputs. There are examples[4] across Government of consultation summaries that include details of how the decision is reached and what evidence is considered. Whilst it may pose a challenge to extend this to technical or scientific issues, it is a challenge worth considering.

What Impact are Departmental Chief Scientific Advisers Having on the Policy Making Process?

It is not clear what the impact across Government has been as there does not seem to be any evaluation following the Cross Cutting Review of Science and Research, or at least no publicly available evaluation. Anecdotally it has been suggested that where the post is well established, or is a senior position, the role can be extremely beneficial and can bring impartial expert advice directly into the department. However, whether this is a universal experience across Government is not clear.

The Cross Cutting Review (2002)[5] recommended:

> "Every department which conducts or commissions an appreciable amount of research, or uses science should have a Chief Scientific Adviser, accountable to the Secretary of State and Ministers for science procurement and advice within the department."

Whilst a number of departments in this category would already have had Chief Scientific Advisers (CSAs), (for instance the Ministry of Defence), is it not clear to us how many departments have since implemented this recommendation. Again, to our knowledge, there does not seem to be a central register of CSAs, nor is there a robust mechanism for assessing the effectiveness of their roles in general.

This lack of monitoring and evaluation of the roles of CSA (and indeed scientific evidence more generally) is a matter of concern to the IEE, and one we raised during Sir David King's review of the Office of Science and Technology Guidelines on Scientific Analysis in Policy making in August 2005 (our comments on evaluation are below).

It is not clear to us how CSAs continue to maintain their contacts and information networks. There do however seem to be simple steps that could be taken to improve the situation. For example, as a professional body, we would be happy to meet with relevant CSAs on a regular basis and such meetings would seem like a sensible method of augmenting and adding value to existing sources.

Treatment of Risk

The issue of risk really centres how it is understood—the problem is in part that "risk" has accepted meanings in science and in popular usage which are significantly different. The general public have also suffered a loss of confidence in "experts", due amongst other things to variety of court cases, which may also contribute to the problems.

The Science Media Centre has a very good publication[6] aimed at scientists and engineers seeking to comment publicly on risk—it explains the gap between the two groups' perceptions extremely well, and offers advice that may even be applicable to Government communications.

---

[4] For example Defra's summary to its consultation on its aims and objectives includes Defra's responses to concerns raised http://www.defra.gov.uk/corporate/aims/summary.htm

[5] http://www.hm-treasury.gov.uk/spending_review/spend_ccr/spend_ccr_science.cfm

[6] http://www.sciencemediacentre.org/risk.htm

The treatment of risk, in a department with a Chief Scientific Advisor, should be common place and built into existing procedures. The communication of this risk should also present no problems, providing advice is taken. There are clear examples in recent history of the poor handling and communication of risk—the examples most commonly given are BSE and GM crops.

Evaluation and Follow-up

We see evaluation as the key factor. Whilst we support the Office of Science and Technology's guidelines, we still believe that the one failing is that of evaluation:

> "As the guidelines are largely principle based, we would encourage departments to ensure they are woven into departmental guidance on better policy making[7]".

It would appear possible for government departments to ignore completely the guidelines, and furthermore, it would appear that there is no monitoring, so this may in fact already be occurring. If strong guidelines exist, should they not be automatically incorporated into departmental policies, and adherence to them monitored?

In our comments to the Office of Science and Technology we suggested that the Consultation Code of Practice could be expanded to include a further principle that the guidelines are used, and that this should be monitored.

Conclusion

The IEE, together with many professional organisations has a wealth of scientific and technical knowledge, and we believe we are well engaged with a number of Government departments. Yet we are still unable to offer any more than an educated guess as to the basis for some decision making (this is not intended as a criticism of all policy decisions).

It seems at odds that whilst a robust set of guidelines already exist, processes to monitor and evaluate their use are not in place. How evidence is used is not monitored, and perhaps most importantly, there is no public scrutiny of the usage—expect for that of this Committee. Nor is the information always made available to the general public.

The treatment and use of scientific evidence must be carefully considered, and public concerns must always been borne in mind. Evidence presented as "scientific" should clearly stand the test of being subject to rigorous standards of scientific method and scrutiny. There may well be reasons that the full decision making and analysis process cannot always be made public, but we do not see any reasons for what we perceive as a lack of evaluation and monitoring of the processes.

January 2006

Annex 1

Areas of scientific or technical advice covered by The IEE

- RFID—Radio Frequency Identification Devices.
- The possible effects on health of mobile phones, base stations and power lines.
- Energy and Environment.
- Health and Safety issues.
- Information Technology including Best Practice Guidelines.
- Safety Related Systems including:
  - Safety Critical Systems.
  - Competency Guidelines for Safety Related Systems Practitioners.
  - Electromagnetic Compatibility and Functional Safety.

www.iee.org/policy

[7] http://www.ost.gov.uk/policy/advice/index.htm

APPENDIX 5

Memorandum from the British Computer Society

1. Executive Summary

1.1 The British Computer Society (BCS) has a strong and positive relationship with the Home Office on the subject of ID cards as detailed below. Such a good example of collaborative working could easily be expanded to other IT related areas. Although not directly associated with the questions asked here, BCS currently provides advice to the Cabinet Office on information security and has strong relationships with Government through EURIM and PITCOM, particularly on the subject of Transformational Government. BCS also endorses the scientific papers submitted by the UK Computing Research Committee (UKCRC).

2. Introduction

2.1 BCS is pleased to respond to the Parliament's Select Committee on Science and Technology Inquiry on "Scientific Advice, Risk and Evidence: How Government Handles Them".

2.2 BCS is the leading professional body for the IT industry. With over 50,000 members, the BCS is the Professional and Learned Society in the field of computers and information systems.

2.3 BCS is responsible for setting standards for the IT profession. It is also leading the change in the public perception and appreciation of the economic and social importance of professionally managed IT projects and programmes. In this capacity, the Society advises, informs and persuades industry and government on successful IT implementation.

2.4 BCS is determined to promote IT as the profession of the 21st century especially as IT is affecting every part of our lives. Therefore, BCS is pleased to take this opportunity to comment on such an important issue.

2.5 In this response, BCS addresses, in particular, the case study of "The technologies supporting the Government's proposals for identity cards", and is therefore providing evidence on the following questions regarding the above-mentioned case study.

3. What Advice Have We Given?

3.1 The following summarizes BCS engagement with policy to date regarding "The technologies supporting the Government's proposals for identity cards":

(a) September 2005—BCS organised a Thought Leadership Debate entitled "Identity Management—a "must have" or a "lost cause".

(b) March 2005—A number of submissions were made on behalf of BCS by BCS members with expertise in the area. BCS was also part of an advisory group which provided input to the London School of Economics interim report on Identity cards (issued in late March 2005). BCS has maintained contact with LSE with a view to a more substantial BCS contribution to the final report.

(c) July 2004—BCS responded to the Home Office Consultation: Legislation on Identity Cards: A Consultation (Cm 6178). BCS Disability Specialist Group also gave written evidence to this Legislation on Identity Cards regarding the use of biometrics in the enrolment process.

(d) May 2004—BCS provided input to the Home Affairs Committee Enquiry into Identity Cards on the draft bill: Legislation on Identity Cards: A Consultation (Cm 6178).

(e) January 2004—BCS provided a statement to the House of Commons Home Affairs Committee enquiry into Identity Cards.

(f) BCS is also actively involved in the ongoing EURIM work on Identity Cards.

(g) BCS dealt directly with the Home Office ID Cards team, taking along a team of experts in the area.

(h) BCS members have been very active in the advisory panels for several Foresight Directorate projects.

3.2 BCS also supported the views which are part of the responses by the UKCRC—an Expert Panel of BCS, the Institution of Electrical Engineers (IEE) and the Council of Professors and Heads of Computing (CPHC), a policy committee for computing research in the UK whose members are leading computing researchers from UK academia and industry. In particular:

(a) December 2005—UKCRC briefing for EURIM Parliamentary members on the National Identity Cards Scheme on the discussion of the technological feasibility of ID Cards set out in the briefing paper written by the ID Technology Advisory Group.

(b) January 2004—UKCRC responded to House of Commons Home Affairs Select Committee Inquiry into the Government's proposals for ID Cards and a National Identity Register. This was followed up with a meeting with the Home Office official managing the ID card project, and then two meetings organised by the Law Society, attended by a Home Office Minister and officials.

3.3 Details or copies of any briefing papers can easily be provided on request.

4. Answers to Specific Questions

Sources and handling of advice

4.1 What impact are departmental Chief Scientific Advisers having on the policy making process?

The impact appears to be continually growing with CSAs expanding their portfolio of knowledge by consulting appropriate advisers, such as the BCS and providing policy based on or influenced by this advice as appropriate.

4.2 What is the role of the Government Chief Scientific Adviser in the policy making process and what impact has he made to date?

The Chief Scientific Adviser should be able to elucidate the evidence that contributes to the debate on policy and appropriately argue where its impact is paramount and the policy in respect of this information as appropriate.

4.3 Are existing advisory bodies being used in a satisfactory manner?

The Science and Technology Reference Group is being used appropriately and BCS advice has been sought, received and welcomed. Naturally there is always room for improvement and the example of ID cards could be expanded to other IT related areas.

4.4 Are Government departments establishing the right balance between maintaining an in-house scientific capability and accessing external advice?

As identified in section 3.2(b) regarding ID Cards this is rapidly becoming much more evenly balance, and as mentioned before this example could be used as an exemplar for other areas.

Relationship between scientific advice and policy development

4.5 What mechanisms are in place to ensure that policies are based on available evidence?

BCS is not aware of such information and is therefore not able to provide any useful feedback.

4.6 Are departments engaging effectively in horizon scanning activities and how are these influencing policy?

From the BCS relationship with the Home Office this is on the increase. A fair amount of amount of good activity is being established by consulting advisers (as detailed above) and also appointing internal Government staff of high quality and capabilities.

4.7 Is Government managing scientific advice on cross-departmental issues effectively?

Experiences from all relationships with Government suggest that cross-departmental issues cause communication barriers leading to a reduction in effectiveness.

Treatment of risk

4.8 Is risk being analysed in a consistent and appropriate manner across Government?

Within the ID arena this seems to have been successful. However in general poor risk analysis and risk management is often identified as a significant factor in the failure of public sector IT-enabled business change projects. Some small areas are handling risk very positively however and this is perhaps a sign of rapid improvement.

4.9 Has the precautionary principle been adequately defined and is it being applied consistently and appropriately across Government?

In the ID card arena, this is a positive area. Such attitude could be easily expanded into other situations and thus improvements made.

4.10 How does the media treatment of risk issues impact on the Government approach?

There is a connection between the media portrayal and Government approaches. BCS has a PR department and from experience BCS suggests that the "connection" is often that "over emphasis on a subject" or "emphasis in a way to cause maximum interest/selling factor" by the media often causes the Government to overreact or react without gathering the precise evidence.

Transparency, communication and public engagement

4.11 Is there sufficient transparency in the process by which scientific advice is incorporated into policy development?

BCS is unable to comment here. There is very little feedback on where the advice influences policy and perhaps if this happened it would be possible to make comment.

4.12 Is publicly-funded research informing policy development being published?

Yes, a great deal of excellent research that could inform policy development is published every year by the academic community. For example, in addition to ID Cards, security information is published.

4.13 Is scientific advice being communicated effectively to the public?

BCS communicates its papers and work on its website and publishes its member magazine, ITNow. UKCRC and other bodies operate in similar ways. However, this could be better coordinated. In addition, the media's appetite for scientific advice is sporadic and tends to focus on post hoc discussions about problems (such as difficulties with the Inland Revenue systems or the Child Support Agency), rather than on policy formation.

Evaluation and follow-up

4.14 Are peer review and other quality assurance mechanisms working well?

The consistency of this is not clear to BCS. There are some areas of excellent practice such as the Gateway reviews. Within BCS, review is a continual process and leads to healthy debate about important topics. The BCS "Thought Leadership Programme" takes a current hot IT related topic and provides a forum for a wide spectrum of influential and intellectual individuals from across society to debate such areas. The data are then collated and utilised as best possible by the BCS. This initiative may be a source of advice for the Government.

4.15 What steps are taken to re-evaluate the evidence base after the implementation of policy?

None are apparent. The response to Question 14 above (the precursor to this) is similar.

5. Conclusion

5.1 The BCS offers advice to Government in IT areas whenever approached. BCS feels that this has been highly successful in the area of ID Cards. However, once advice has been offered there is a lack of feedback or follow through process. BCS would recommend that the whole area of feedback/follow through is reviewed with new processes identified and put in place. Where such advice actually informs policy those involved should be acknowledged and communicated with to ensure full understanding of the advice given,

5.2 The follow through once this advice has been offered however, seems to be a little lacking. Therefore BCS recommends that this whole area is considered and new processes put in place where such advice may genuinely inform policy and those involved both acknowledge and understand the advice given.

5.3 The example of ID Cards can be an exemplar for other areas of activity and BCS wishes to assist in whichever appropriate way Government recommends.

January 2006

APPENDIX 6

Memorandum from Dr John Daugman, University of Cambridge

INQUIRY ON USE OF SCIENTIFIC EVIDENCE IN POLICY FORMATION AND ASSESSMENT

Executive Summary

Public discussion of scientific issues related to biometrically-enabled ID cards has been of poor standard. This is because public debate about the proposed biometric ID cards has been dominated by a single document, the "LSE Report," which had no natural scientists amongst its putative or actual authors. Persistent errors of fact are repeated both in that Report and in the parallel press campaigns run by its organisers. This Memorandum documents some of the misinformation and recommends that in future the broad scientific basis for policy proposals should be assembled in an on-line web resource containing balanced and critical empirical documents. This may prevent future hijacking of public discussion by scientifically misinformed assessments that are spearheaded by activists under academic cover.

1. I thank the Science and Technology Committee for inviting my comments about the way in which the Government obtains and uses scientific advice, specifically in connection with the proposals about identity cards. The aspect on which I wish to comment is the way in which the public debate, and to a significant extent the Parliamentary debate, on this issue has been influenced by scientific misinformation from lobbyists opposed to the proposals. In some cases (which I will document here) it could even be called disinformation. Of relevance under the Terms of Reference of the present Inquiry is whether such tactics have influenced policy formation or assessment, and whether in its public communications the Government has adequately challenged the scientific misinformation.

2. Immediately prior to every Reading of the ID cards bill in either House, a report ostensibly prepared by senior academics at the London School of Economics was widely disseminated. The putative LSE authors included no scientists. Moreover the LSE Reports were spearheaded and apparently written not by the LSE Professors whose names appear on them, but by Simon Davies, who is Director of Privacy International, a political lobbying organisation fiercely opposed to the concept of citizen identification.

3. Although recent debate has shifted mainly to questions of cost, a major focus earlier was the scientific and technical feasibility of biometric identification of persons across a national database. Both the LSE Report and a wider press campaign by the same source to influential media (including *The Economist*; *New Scientist*; and the broadsheets) asserted repeatedly that biometric identification simply would not and could not work. Arbitrary statistics about False Match rates were fabricated from thin air and presented as scientific facts in that media campaign, contradicting all available scientific evidence, as I shall detail more fully in paragraph 9.

4. However ambiguous or contrived may be the authorship of the LSE Report, the absence of any natural scientists from amongst even its putative authors may explain the persistent errors of scientific fact that appear within it. Many of these arise from confusing the iris with the retina. (The iris lies near the front of the eye, in front of the lens. The retina lies at the very back of the eye.) These simple errors when assessing the feasibility of the iris biometric, for example if the lens of the eye becomes cloudy from cataract, occur equivalently both in the "Interim" release of the LSE Report dated 23 March 2005 and in its final release dated 27 June 2005, and so henceforth I shall refer to both releases collectively as "the LSE Report."

5. Glaucoma, diabetes, cataracts, blindness, and pregnancy were all incorrectly said to affect the iris pattern, or its visibility: "People with glaucoma or cataracts may not be reliably identified by iris recognition systems." "People with diabetes . . . will not be able to use this biometric method." In fact glaucoma affects the retina, not the iris. Cataract clouds the lens, which lies behind the iris and which therefore does not affect the visibility of the iris. Diabetes may affect the retina, not the iris.

6. It is informative to trace the origins and promulgation of so many basic misunderstandings. Invariably in the biometrics debate the sequence is that statements which began as speculation or simple errors in earlier reports or in the press, become cited as established facts in later documents without further investigation. This is the ubiquitous standard of scientific evidence in the LSE Report. For example it is taken for granted that blind persons, or those with visual disabilities, must lack eyes or lack visible irises. (The blind former Home Secretary David Blunkett successfully used an iris recognition system.) When I pursued one such confusion about eyes with the authors of a document submitted to the Commons Home Affairs Committee by the British Computer Society, I learned that they further believed that the iris "shatters at birth."

7. Most bizarrely, the LSE Report asserts that "Pregnancy . . . can affect the recognition of irises;" and that "Patterns in the eye may change over time because of illness," and that "using the iris image for health diagnostics" is a concern. This practice, and these beliefs, are called Iridology. All published scientific tests

of Iridology (see bibliography at http://www.CL.cam.ac.uk/users/jgd1000/irido1ogy.htin1) have dismissed it as medical fraud. Yet this belief in systemic changes in iris patterns seems to be part of the basis for the LSE high cost estimate for the ID cards scheme, as the Report asserts that the biometrics would need to be re-enrolled frequently for these reasons.

8. Besides scientific inaccuracies such as those cited above, the influential LSE Report was extremely selective in the data that it cited. It ignored completely the very positive test data about large-scale biometric capabilities reported for example by the US National Institute for Standards and Technologies. In particular, it ignored eight published studies conducted over the past decade about the accuracy of iris recognition, each one finding no False Matches. Two of those reports were particularly germane to the contemplated large-scale UK deployment, as they showed that with reasonable thresholds it was possible to perform two billion iris cross-comparisons without making any False Matches (IBG ITIRT Report 2005); and indeed 200 billion iris cross-comparisons were performed without encountering any False Matches (University of Cambridge Technical Report UCAM-CL-TR-635, 2005). The origin of such resilient performance is the mathematical principle of binomial combinatorics embedded into the iris recognition algorithms, a topic which again has eluded any public discussion. The scale of this huge number of iris cross-comparisons (200 billion) without making False Matches is not widely appreciated. It is larger than the estimated number of stars in our galaxy; it is larger than the estimated number of galaxies in the universe; and it is larger than the estimated number of neurones in the human brain.

9. Yet in earlier phases of the campaign against ID cards, several influential journals (including *The Economist* and *New Scientist*) and press were told by the organiser and author of the LSE Report that iris recognition has a "False Match Rate of 1%;" that "for every 100 scans, there will be at least one False Match," and that therefore in a nation of 60 million persons, "each person's scan will match 600,000 other records in the database." (Simon Davies, *New Scientist* 180, no 2422, page 13.) This statistic was simply conjured out of thin air with no basis in fact, and obviously it contradicted dramatically all of the above-mentioned studies. Nonetheless it was published as a fact without further investigation.

10. Every day today some seven billion iris comparisons are performed in a national security deployment covering all 27 air, land, and sea ports of entry into the United Arab Emirates, comparing arriving passengers against a central database of iris patterns. (About 9,000 daily arrivals are each compared by real-time exhaustive search against an enrolled database of 800,000 IrisCodes, making 7.2 billion iris comparisons per day.) According to the UAE Ministry of Interior, over the past 4.5 years this system has caught some 50,000 persons trying to enter or re-enter the UAE under false travel documents. If the putative 1% False Match rate were correct, then the daily volume of seven billion iris comparisons would be producing 70 million False Matches per day. If this were true, I should have thought someone would have noticed.

11. Both the LSE Report, and the parallel media campaigns arguing that biometric identification cannot work, have been highly influential. The Leader of the Opposition, David Cameron, stated on 15 January 2006 (BBC, Andrew Marr's Sunday AM Programme) that he based his objection to the ID Card proposals primarily on the LSE Report's conclusion that the system would be unworkable. Commons MP and Home Affairs Select Committee member the Rt Hon Bob Russell (Lib Dem) declared that iris cameras would cause epileptic fits, and that trained medics would need to be standing by at each one. *New Scientist* (180, no 2422, page 13) asserted that the iris is a kind of thermometer, changing its pattern with temperature. The conclusion of the LSE Report about the technical feasibility of biometrics (page 184) was that "Implementing biometrics [in the UK] could bring the country to a standstill."

12. Conclusion: The science of biometric pattern recognition and its underlying mathematics has been not only ignored but contradicted and overwritten by political campaigners against the Government's ID cards proposals. In effect this important part of the discussion has been hijacked, as have also been some academics. Under these unusual circumstances, with public debate so steered by a scientifically misinformed document and a parallel press campaign, the public interest may have been better served by a more robust presentation from Government of the scientific basis and technical capabilities of biometrics. One mechanism whereby this might be achieved in future would be to create and maintain an on-line website resource containing a balanced and critical collection of scientific papers and reports that inform and address public policy proposals.

January 2006

APPENDIX 7

Memorandum from QinetiQ

QinetiQ is Europe's largest integrated research and technology organisation, with over 9,000 employees in the UK, more than 750 of them PhDs. Formed from the Ministry of Defence's research, development and testing agencies and now in the market place, QinetiQ generates world-class technologies that are applied not only in the fields of defence and security but in aerospace, financial services, health care,

transport and the environment. QinetiQ has a long tradition of tendering impartial and respected advice to UK Government departments and agencies, and as a contractor to government is also subject to the scientific advice received by Departments from a wide range of other sources.

QinetiQ has an involvement in all three of the areas selected as case studies by the Committee, but most deeply in the field of ID card technologies, to which most of our observations relate. We also have a couple of general points to make. In view of the brevity of our evidence, we have taken the liberty of dispensing with an Executive Summary.

General Points

1. We fully support Sir David King in his drive to ensure that decisions in all Government departments are taken on the basis of high-quality scientific advice. The Departmental Chief Scientific Advisers are starting to make their presence felt, some more quickly than others depending on the culture of different departments.

2. The term "scientific" tends to be drawn too tightly. It is important that government and its agencies receive not only the best scientific advice, but technological advice of a similar calibre. This is not always fully appreciated at present.

The National Identity Card Programme

Sources and handling of advice

3. In programmes such as CBRN the influence of the Government Chief Scientific Adviser has been very clear. However, for the NICP, the impression given is that most of the policy has been driven by the results of technology assessments from outside government and outside the Home Office.

4. There is little evidence that the Chief Scientific Adviser has had any influence on the ID Card programme, not least since there appeared to be some duplication in technologies being sought between the NICP and eBorders programme. These are two very similar programmes, with similar aims, being run by two different departments within the Home Office with no apparent coherence although it would be fair to recognise that matters have improved over the past nine months.

Are existing advisory bodies being used in a satisfactory manner?

5. The Home Office has used the National Physical Laboratory in its earliest soundings of appropriate technology for NICP, but QinetiQ, in its advisory capacity, has been surprised that our involvement with similar biometric programmes conducted on behalf of the Home Office and other Departments has not been sought.

Are Government departments establishing the right balance between maintaining an in-house scientific capability and accessing external advice?

6. Although we are accustomed to the very structured approach to R&D and procurement adopted by the MoD, the Home Office's reliance on S-CAT and University research seems to miss the depth of experience and expertise available in the UK defence industry, a resource which is more familiar with the challenges of large scale programmes and could guide the Home Office on managing innovation into major projects.

Relationship between scientific advice and policy development

Are departments engaging effectively in horizon scanning activities and how are these influencing policy?

7. In the case of the NICP, we were surprised that no activity was undertaken to look at technology lifespans over the duration of the expected programme, with a view to understanding vulnerabilities that will arise as technologies become obsolete and vulnerable to criminal exploitation.

Is Government managing scientific advice on cross-departmental issues effectively?

8. There are two issues to be addressed here: the effective management of scientific advice on issues affecting more than one department, and the need to make sure that effort on differing programmes within a department is not duplicated.

9. Within the Home Office, the similarity and possible duplication of effort in NICP and eBorders suggest that cross-departmental issues and projects could be managed more effectively, although it is accepted that this particular duplication may be a one-off instance.

Treatment of risk

Is risk being analysed in a consistent and appropriate manner across Government?

10. It is our view that the programme still contains considerable risk at this stage of procurement, even though the Bill under which it is due to operate is well on its way through Parliament. Although the outline business plan—not available in the public domain—has clearly costed the system, it has not done so from the standpoint of a telecommunication system and sized the system, and thus the programme, by data size and data transmission. This suggests to us that the programme is not being costed or scaled on a basis more normal to standard communication engineering practices.

How does the media treatment of risk issues impact on the Government approach?

11. It inevitable that the media will focus on the sensational or the worrying stories. More attention needs to be given upfront to combining a media-savvy approach with informed technical input. Unless acceptable risk is presented in an intuitively understandable manner then the project can suffer from either excessive conservatism or it becomes vulnerable to media drive alarms.

Transparency, communication and public engagement

Is there sufficient transparency in the process by which scientific advice is incorporated into policy development?

12. There is probably sufficient transparency by now on this issue, and the situation continues to improve. Unfortunately, at the beginning of the programme, available information and justification for activity appeared thin.

Is publicly-funded research informing policy development being published?

13. In some areas of the NICP, scientific advice has been used to support policy. However, on scrutiny the evidence has been more limited than the claims made for it. In addition, much of the information made public so far has been published after policy has been made, and has not been used to inform debate or comment.

Is scientific advice being communicated effectively to the public?

14. The technology aspects of the NICP could be better used to justify policy action. QinetiQ has undertaken considerable work for government on various aspects of identity management. We were surprised that much of this was not utilized and, instead, a single report from the National Physical Laboratory—valid though it was—was the sole justification for using three biometrics, for instance. The case could have been stronger by tapping into the archive of technology reports that existed in Government and elsewhere.

Evaluation and follow-up

Are peer review and other quality assurance mechanisms working well?

15. In the case of the NICP, this process is not visible to QinetiQ.

What steps are taken to re-evaluate the evidence base after the implementation of policy?

16. Some re-evaluation is now being undertaken within NICP to further risk reduce the programme in the light of the very short procurement period that is provided for after the Bill is enacted. Although an earlier re-evaluation of procurement strategy would have improved the procurement strategy, it would probably not have affected policy.

February 2006

APPENDIX 8

Memorandum from the London School of Economics and Political Science Identity Project Team

Executive Summary

1. This submission presents the experience of the LSE Identity Project team on the government's use of scientific and technological advice on the Identity Cards scheme. The team has identified areas of concern with the way that the government uses this advice in almost all aspects of the project; indeed we would suggest that this project would be an ideal candidate for how not to use scientific and technological advice for building a large scale, complex project[8].

2. The biometric technology at the core of the scheme has been untested at the scale proposed by the Home Office, the database with the details of every ID card holder is likely to become a significant target for security attacks, and the practicalities of implementing the ID cards scheme across government and the private sector have all been questioned by scientific and technological experts. Very little of this expert advice appears to have had any impact on the shape of the ID cards scheme and it would seem that the Home Office is intent on short-cutting any discussion of this expert advice in favour of its own particular conclusions: the technology will work and achieve its aims.

The LSE Identity Project

3. Many departments at the LSE have played prominent roles in academic and policy circles on issues relating to information policy. The LSE Identity Project is another such initiative to generate understanding and inform policy debate and deliberation. For decades the London School of Economics has been conducting research on a wide variety of pressing policy issues. LSE staff advise governments, serve on Royal Commissions, public bodies and government inquiries, and are seconded to national and international organisations. In the past three years alone, the LSE has conducted research and analysed policies in over 70 different projects commissioned and funded by a variety of UK Government departments and agencies amounting to more than £11 million.

4. The Department of Information Systems began its research into authentication and identification systems in the 1990s. In 2003 it decided to conduct research to inform policy deliberation on biometric identification systems. Subsequently, the Department began a concerted initiative to inform the debate on the proposed identity card, first by hosting a number of public meetings on the then "entitlement card", then convening meetings with industry leaders and government departments. In 2005 this research activity culminated in the LSE's "Identity Project".

5. Over 100 researchers and experts in technology and policy contributed to the project's two reports over a concentrated period of months. The results were a 300 page *main report* issued in June 2005 and a follow-up 55 page research *status report* issued in January 2006[9]. The reports questioned some of the key policy goals of the ID cards scheme, reviewed the likely effects on policing, assessed the challenges and risks in the Government(s proposals, and offered an alternative scheme for public consideration.

6. As well as contributing directly to the policy process through criticism, advocacy and deliberation, members of the Identity Project have an ongoing academic interest in the policy development process, especially as it relates to technological issues and technological expertise. Our submission therefore aims to assist the Committee in its work on these important issues and we particularly draw to the attention of the Committee to two sections of our *status report*: The research challenges that we identify in section II and the unanswered questions presented in section III.

7. In presenting our points, we draw on detailed evidence presented in our two reports as well as wider evidence, but do so not to replay issues that have been scrutinised in parliamentary debate but rather to raise those methodological concerns we have noted during this study.

8. The remainder of this submissions is structured as follows. We next outline the research philosophy that underlies our work, before addressing the five areas of concern specified in the committee's terms of reference. For each of these areas, we highlight particular examples of problems that we discovered during our analysis of the government's Identity Cards scheme.

---

[8] This view is shared by the IEEE *Spectrum* magazine, which named the ID cards scheme one of the worst technology projects in 2006. "Why It's a Loser: The design of the system is based on unreliable and inadequate technologies that could result in privacy and security problems." See http://www.spectrum.ieee.org/jan06/2597.

[9] Electronic copies of these reports, plus associated press releases and links to press coverage are available at http://is2.lse.ac.uk/IDcard/default.htm.

Research Philosophy

9. A number of members of the Identity Project have particular research interests in understanding the relationship between technology and society and their relationship to policy deliberation[10]. Others have research interests in the management and implementation of large IT projects, including government IT projects[11].

10. In our research we have drawn heavily on theories that emphasize the role that social factors play in the shaping of technological artefacts as well as the work of Bruno Latour on the nature of scientific facts. His recent book on the politics of nature[12] has been particularly influential. In this work (which is focussed on scientific results about "nature" but presents an argument that can equally be applied to "technology") Latour raises concerns about "due process" in incorporating scientific results for public policy issues, especially when the scientific results are currently uncertain. Recent examples of such uncertainty in science include global warming and BSE. In a similar manner, we would argue that there is also considerable uncertainty surrounding most aspects of the ID cards scheme.

11. Latour starts from the distinction between "facts" and "values" and notes that, in both cases, they are made up of two distinct activities. What we commonly understand to be scientific or technological "facts" are actually the result of a process whereby we start with "perplexities" ("Do greenhouse gases contribute to global warming?") and end up with institutionalised agreements of accepted truths ("Gravity exists and has these properties"). A similar two part process applies to values, which he suggests can be understood in terms of activities of consultation and hierarchy.

12. From these distinctions, Latour argues that we need to be careful to ensure that due process is followed in moving from perplexities to institutionalised truths. In particular, he is concerned about short-cuts being taken whereby perplexities become institutionalised truths without undergoing due process. For example, moving from perplexities about the scalability of biometrics systems to the truth that the technology exists and is suitable for use in the ID cards scheme. He proposes a model by which due consideration is given to perplexities through processes of consultation and hierarchy, some of which are incorporated into responses (institutionalisation) at a particular time, before repeating the process with new perplexities and considerations in the next time frame. See footnote 13 for an application of this model to policy debate around technological issues.

13. More generally, we recognise the difficulties that any policy deliberation process faces when dealing with scientific and technological advice, especially at the early stages of understanding of new phenomena when there is no "independent arbiter" to call upon to resolve differences of opinion. From a policy perspective, we believe that an open, informed debate that actively encourages alternative perspectives and analyses is vital for ensuring that such debates are not short-cut by particular bodies with particular interests.

Sources and Handling of Advice

Don't shoot the messenger

14. On publication of the LSE Identity Project reports, many experts contacted us with their ideas, comments and suggestions. We received a high level of interest from Parliamentarians, industry representatives, technology and policy experts and members of the general public from around the world. What we were not expecting, however, was the response from Government officials and Ministers, many of whom launched spurious, misleading and *ad hominem* attacks on the reports and its authors. We detail these attacks, and our repeated responses to them on page 2 of our status report.

[10] For example, Hosein I (2004) The Sources of Laws: Policy Dynamics in a Digital and Terrorized World. *The information society* 20(3), 187–199; Hosein I and Whitley E A (2002) The regulation of electronic commerce: learning from the UK's RIP act. *Journal of Strategic Information Systems* 11(1), 31–58; Whitley E A and Hosein I (2005) Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications Policy* 29(11), 857–874.

[11] For example, Angell I O and Demetis D (2005) Systems thinking about anti-money laundering: considering the Greek case. *Journal of money laundering control* 8(3), 271–284.; Dunleavy P, Margetts H, Bastow S, Bouçek F and Campbell R (2003) *Difficult forms: How Government agencies interact with citizens.* (NAO), Report HC 1145 Archived at http://www.nao.org.uk/publications/nao_reports/02-03/02031145.pdf; Margetts H and Dunleavy P (2002) Better public services through e-government.; Sauer C and Willcocks L (2001) *Building The E-Business Infrastructure*. Business Intelligence, London.; Willcocks L and Griffiths C (1997) Management and risk in major IT projects. In *Managing IT As A Strategic Resource* (Willcocks L, Feeny D and Islei G eds.) McGraw-Hill, Maidenhead; Willcocks L, Petherbridge P and Olson N (2003) *Making IT count: Strategy, delivery, infrastructure*. Butterworth, Oxford.; Willcocks L P and Kern T (1998) IT outsourcing as strategic partnering: the case of the UK Inland Revenue. *European Journal of Information Systems* 7(1), 29–45.

[12] Latour B (2004) *The politics of nature: How to bring the sciences into democracy*. (trans Porter C) Harvard University Press, Cambridge, MA.

[13] Whitley E A and Hosein I (2001) Doing politics around electronic commerce: Opposing the Regulation of Investigatory Powers Bill. In *Realigning Research and Practice in IS Development: The Social and Organisational Perspective* (Russo N, Fitzgerald B and Gross J I D eds.) 415–438, Kluwer, Boise, Idaho.

15. Throughout this time, we have had the unwavering support of the Director of the LSE and the LSE Council, who have strongly defended "the right of any member of the School to contribute to areas of public policy development in which they had expertise". See footnote 14 for a recent example of this support. This support was invaluable to us and there is a real risk that other researchers might not receive such support in response to similar attacks on the reputation of their institution.

Policy Laundering

16. Elsewhere[15], we have defined policy laundering as "a practice where policymakers make use of other jurisdictions to circumvent national deliberative processes". This has been particularly noticeable in the debates about the ID cards scheme, where ministers have continually referred to "international obligations" for passports and travel documents, drawing on internationally agreed standards defined by the International Civil Aviation Organization (ICAO).

17. The Home Office has repeatedly claimed that ICAO requires the introduction of biometric passports and that, if the identity cards are to be used as travel documents, they must meet these requirements.

18. As we made clear in our briefing note to the House of Lords[16], there are significant differences between ICAO requirements and the proposed use of biometrics for the ID cards scheme. Amongst the key differences are the number of fingerprints taken, whether templates are taken of the face and iris, or if they are just stored as images.

Relationship Between Scientific Advice and Policy Development

Design of the system

19. There are many ways to design even the simplest technologies that will cause a significant difference in outcome for society. Whether it was the intention of the designer, early applications and market opportunities, the social norms at the time, or a myriad of other factors, small decisions can transform the way our society works.

20. We noted in our main report (chapter 18) that "the controversy, challenges and threats arising from the Government's identity proposals are largely due to the technological design itself" and "some of the larger decisions regarding the architecture of the scheme are already decided, and are encoded within the bill".

21. Relatively simple choices, such as which department or ministry is responsible for the design of a government infrastructure, may radically shape future policy decisions, and may even determine entire courses of action.

22. When the Home Office is the proponent and selector of an infrastructure as vast as an identity system, the choices made in the basic design of the system will reflect the interests and expertise of the Home Office. This is particularly important in the design of an ID scheme, given that its design goals include not only combating crime, but also enabling e-government, enhancing trust in commerce, and providing the "gold standard" for identity in Britain. The Home Office's design choices are in stark contrast to the system being developed in France, emerging from the Ministry for the Civil Service, State Reform and Spatial Planning. The ID Card Bill for the UK proposes a massive complex centralised system with an audit trail that focuses on identification, while the French system proposes a simpler decentralised and user-oriented system that focuses on confidence-building.

23. In other areas, however, the Home Office appears to be much more flexible with proposed details of the system. For example, it has recently proposed the use of a web portal for viewing / verifying the audit trail details held on the NIR and the use of chip-and-PIN authentication and one-time passwords for verification if biometrics are not to be used to verify that the person presenting the card is its true holder. We are unaware of any costings or market soundings about these particular technological developments.

The status of expert advice

24. The parliamentary debate about the ID cards scheme has demonstrated an inconsistent usage of expert advice by the Home Office. Where advice appears to support the Home Office position, it is accepted without question and contrary evidence from the same source is overlooked. For example, on 15 November 2005 Baroness Scotland referred to a study by the US National Institute of Standards and Technology and claimed that this work, which had a sample size of six million fingerprints and used data collected in operational circumstances, "showed a performance consistent with the needs of a scheme on the scale of the ID cards scheme". Ignoring the fact that we are "still" unaware of the particular study that made such strong

[14] http://news.ft.com/cms/s/d429d28c-945a-11da-82ea-0000779e2340.html.

[15] Hosein I (2004) The Sources of Laws: Policy Dynamics in a Digital and Terrorized World. *The information society* 20(3), 187–199.

[16] LSE Identity Project (2006) *All party Briefing for report stage.* Report Archived at http://is.lse.ac.uk/IDcard/VolCardBriefing.pdf.

claims for the reliability of the technology in operational circumstances, another NIST report states that many of the problems with misidentification of biometrics can be attributed to "lower operational quality controls" during the collection process[17], ie that there are likely to be very real operational issues associated with the rolling out of the biometric enrollment and verification process.

25. On other occasions, the Home Office appears to take the most positive reading of the available evidence to support its case. For example, on 23 January 2006, Lord Bassam said "The identity card programme has been through, and completed, an extensive market sounding and card durability survey with leading international card and chip manufacturers. The manufacturers confirmed that a card life of 10 years *is viable* and provided evidence where they have guaranteed that card life" (emphasis added). ICAO have suggested that "States may wish to consider setting the maximum validity of their travel documents to five years"[18]. Amongst the reasons they give are: "Most Chip applications assume a chip/smartcard validity of two to three years—how such technology will perform over five to 10 years is yet to be tested in real world applications as the technology typically has not been deployed with consumers for that length of time". Given that the cost of issuing replacement cards is a relatively minor aspect of the whole programme, the Home Office insistence on this point is rather puzzling.

26. The ICAO also suggests a five year validity period for travel documents because "Biometrics technology is changing at a rapid rate, so a shorter validity period enables re-enrolment using more sophisticated technology" and "Performance of biometrics can tend to decline over time (eg compare 10 year old photographs vs five year old photographs)"[19]. Contrast this with the Home Office response to the LSE alternative blueprint which stated "Quote from the National Physical Laboratory report 'Feasibility study on the use of biometrics': 'in the case of facial recognition it would seem advisable to update the templates at least every 10 years. Fingerprints and iris should be considerably more stable'. Thus, we would not need to retake biometrics for the majority of citizens during the 10 year validity period of their passports"[20]. Retaking biometrics for a large proportion of the population is likely to be costly, which might explain the political choice for ignoring this alternative reading of the evidence.

Radio Frequency Identification (RFID) tags

27. This issue about the nature of the chip on the ID card has arisen recently and suggests some confusion about the adoption of ICAO standards. For a full explanation of the consequences of this confusion, see[21].

28. On 7 December 2005, Andy Burnham gave a written answer stating "The identity card scheme will secure information on the identity card through a number of methods, including the use of anti-skimming technology. The identity cards programme has reviewed technical methodologies for anti-skimming measures for contactless cards which are compliant with International Civil Aviation Organisation (ICAO) recommendations for machine-readable travel documents" [32084] but on 13 December 2005, the Minister gave a written answer stating that "There are no plans to use radio frequency identification tags in ID cards" [32082]. However, on 10 October 2005, the Minister gave a written answer that said "We are considering the use of 'contactless chips', which contain radio frequency chips" [9551].

Treatment of Risk

System implementation

29. In our *status report* (page 18) we noted that "the accumulated independent evidence on large complex IT projects is that they have been and always will be high risk in terms of implementation and unanticipated costs. The key risk dimensions include high complexity, large size, innovativeness of technology, integration issues, number of units and stakeholders affected, over-ambitious time-scales, and over-reliance on technologists/IT suppliers for development and implementation". A similar point was made in a recent report from the House of Commons Committee of Public Accounts[22].

30. One way of addressing public concerns about such risks would be to include explicit statements of what the project team does not know, and what the major risks are, in all major policy documents. Similarly, they should make explicit a variety of alternative scenarios for pessimistic, medium and optimistic outcomes in all documents, instead of simply providing confident statements of costs and benefits at the front end.

[17] NIST (2005) *The Myth of Goats: How many people have fingerprints that are hard to match?,* Report NISTIR 7271 Archived at http://www.itl.nist.gov/iad/894.03/pact/ir_7271.pdf

[18] ICAO (2004) Biometrics deployment of machine readable travel documents.(ICAO), Report Archived at http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf Page 47

[19] Ibid

[20] Home Office (2005) *Home Office Response to The London School of Economics' ID Cards Cost Estimates & Alternative Blueprint.* Report Archived at http://www.identitycards.gov.uk/library/Response_LSE_Alternative_Blueprint.pdf

[21] The Register (2006) *"RFID tag"–the rude words ID card ministers won't say.* Report Archived at http://www.theregister.com/2006/01/30/burnham_rfid_evasions/

[22] House of Commons Committee of Public Accounts (2005) *Achieving value for money in the delivery of public services.* Report HC 742 Archived at http://www.publications.parliament.uk/pa/cm200506/cmselect/cmpubacc/742/742.pdf

31. Despite the "design" of the ID cards scheme having been fixed as early as 2002 there is a growing concern from industry about the lack of openness about the implementation of the ID cards scheme. For example, EURIM notes that *"None of the potential suppliers have had sufficient access to specification of what is intended or who is to be served to be able to provide costings of any reliability.* There is no evidence that the potential private sector partners with experience of running supposedly similar operations (eg financial services) have been consulted in any more depth" (emphasis added). They continue: "The experience of financial services industry security experts on the attitudes and experience of others they met at an open consultation meeting suggest that there is a gulf of understanding between those running systems under regular and sophisticated attack and those who are not under such pressures."[23]

32. In a similar manner, Intellect, notes that "far more discussion is still required before Government will be in a position to make informed decisions on all of the proposed technologies including biometrics, but also data management, security, authorisation/authentication, storage and data sharing between departments. The only way that Government will be able to develop an ID Card scheme built on reliable technology and capable of delivering on its promises to citizens will be if it has a comprehensive understanding of the industry, its capacity and its capabilities. Regarding the technology which will enable the project it is industry's belief that the scheme should be built on technology and business processes that have been proven in existing implementations around the world. And that the only way that Government will achieve this is by talking to industry, *being honest about their requirements*, and listening to industry's advice" (emphasis added).[24]

The ID cards scheme as an infrastructure

33. Since it was first proposed in 2002, the Identity Cards proposal has failed to win universal support amongst central government departments. The Home Office intended the ID cards scheme to provide a gold-standard identity infrastructure for use by all government departments and one would expect that if these other government departments were confident of the Home Office's ability to deliver the scheme successfully they would have no problem being compelled to integrate their own systems with the ID cards scheme. However, the present Bill places no obligation on departments to make use of the scheme.

34. Not mandating the use of the ID cards scheme across government suggests major concerns with the project and goes against the stated government policy of providing joined up government. Furthermore, despite a three and a half year marketing effort to the rest of government, the Home Office has failed to achieve formal buy-in to the scheme, with most Departments and agencies responding to a series of Parliamentary questions, posed to clarify this matter, using a fairly standard, non-committal answer, typically of the form that the Department in question "has, in consultation with the identity cards programme, developed its current best estimate of the costs and benefits of using the ID cards scheme to enhance its services and these have been incorporated into the business case".

35. The distinction between infrastructures and stand-alone systems helps explain, in part, the discrepancy in cost estimates between the LSE and the Home Office. Our figures always included set-up costs, running costs and costs of integration with other Departments. The Home Office figures, we now understand, are "The current best estimate for the total average running costs for issuing passports and ID cards to UK nationals is £584 million per annum. The Home Office is not breaking this cost down further, *nor publishing details of set-up costs,* because this information is commercially sensitive and discussion of more detailed estimated costs may prejudice the procurement process by limiting the Department's ability to secure value for money from the market" (emphasis added). [21354]

Untested technology

36. For the project to work, a relatively new and untried technology has to be made to work, and known shortcomings have to be resolved. The government was relatively late in starting to spend any money on investigating how well the technology actually works and what needs to be done to overcome current limitations. There is a significant risk that the technology will never work well enough in practice for a large-scale public domain application, and large amounts of money will be lost if this is discovered too late in the project.

37. We have been repeatedly struck by the deep-seated, fervent belief, held by ministers and top project team members, that the technology can be made to work. This belief is literally unshakeable. However, the basis for this confidence is unclear (unless it is based on companies telling them that they can fix current shortcomings). When ministers are pressed on this point, they typically resort to avoiding the question and restating the fact that strong identity management is needed and that something must be done in this area.

[23] http://www.eurim.org.uk/activities/pi/060112pireport.pdf
[24] http://www.intellectuk.org/press/pr/pr_190106—id_card_debate.asp

Transparency, Communication and Public Engagement

Purpose of the system

38. The reasons given for the introduction of the NIR and use of biometrics do not hold when even a basic risk analysis is conducted as a closer inspection shows that identity only plays a small role in many of the issues raised. This is particularly evident in press comment about the recently updated "figures" for identity fraud.[25] For none of these cases has the government presented a complete solution required to tackle it, so that a proper cost-benefits analysis case for the NIR can be undertaken. Indeed, in the worst case, identity cards could actually reduce the ability to deal with the listed problems, because too many resources have been spent in this area to the detriment of other activities.

Consultation

39. Issues of design become particularly important when seen in conjunction with the formal consultation process that has been undertaken by the Home Office. All of the consultations to date raised concerns and observations regarding law, social exclusion and technology, as we detailed in chapter 5 of our main report. Few of these have been reflected in the final bill. In fact, we noted, "the government's plan for the ID card has changed little since the beginning of its gestation". The first Home Office consultation document, issued in 2002[26] (using the term "entitlement cards") presents the design of the scheme as a central database, secure procedures for establishing entries on the central register and for keeping the information up to date, links between the central register and information held on other systems and the issuing of plastic cards to everyone on the central register.

Responses to consultation

40. We noted in our main report (pages 33–34) that as part of the formal consultation process, the lobby group Stand.org.uk set up a portal to allow people to send their comments to the Home Office easily. This resulted in 5,031 responses, overwhelmingly against the Scheme. In its review of the consultation process, the Home Office appeared to count these 5,000+ responses as a single response arising from an organised campaign and hence was able to claim that 61% of responses to the consultation were positive.

Formal reviews

41. We understand that the ID cards scheme has undergone two formal OGC gateway reviews and that the methodology used for costing the project has been assessed by KPMG.

42. We note, however, that neither of the reports (or even the "scores") for the OGC gateway reviews have been released and the KPMG report was only released as an "extract". There might be good reasons, in terms of enabling a full, frank and open reflection of possible problems with the project at the time, for keeping the details of the OGC reviews private, however, the Home Office's continued reliance on the reason of "commercial sensitivity" for failing to reveal this information is doing little to improve public confidence in the scheme.

Evaluation and Follow-up

Technology neutral policy

43. The question of whether to go for technology neutral policy is an important one for legislators. A technology-neutral policy has the advantage of not needing to be updated whenever there are significant changes to underlying technologies. The disadvantage, as we have argued elsewhere,[27] is that all too often, technological issues are fundamental to the way the technology is understood and regulated. For example, arguments about the regulation of e-mail are very different if one is considering SMTP communications (as used in most e-mail packages) versus HTTP communications (as found in hotmail and googlemail, which are based on web browsers). It appears that the Home Office's plans to address this issue has been to specify

[25] "To support the claim of the £1.7 billion 'cost' of ID fraud, the Government cites a figure of (£395 million 'lost' to money laundering. But on closer examination, it turns out the Government has no idea how much money is laundered, or indeed how much of this is directly attributed to identity fraud. The figure on which a minister of the Crown is talking on national radio, it turns out, is entirely 'illustrative'. The figure of £1.7 billion becomes even more ridiculous when you realise that it assumes a zero level of ID theft once cards are introduced, when there are good arguments to suggest the scheme will actually make ID fraud much easier for sophisticated criminal gangs" A £1.7 Billion red herring. Comment, *The Daily Telegraph*, 3 February 2006.

[26] http://www.identitycards.gov.uk/library/entitlement_cards.pdf

[27] Hosein I, Tsiavos P and Whitley E A (2003) Regulating Architecture and Architectures of Regulation: Contributions from Information Systems. *International Review of Computing Law and Technology* 17(1), 85–97. Whitley E A and Hosein I (2005) Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications Policy* 29(11), 857–874.; Hosein I and Whitley E A (2002) The regulation of electronic commerce: learning from the UK's RIP act. *Journal of Strategic Information Systems* 11(1), 31–58.

the broad design in the legislation, but leaving much of the technological detail to secondary legislation, much of which has not been introduced yet, a point also raised by the House of Commons Home Affairs Committee.[28]

The sense of inevitability

44. The Home Office, and at times the Prime Minister, have pushed the notion that the identity cards policy is inevitable. The purpose of this imagery is to indicate that Parliament's consent to this scheme is merely a formality and a re-affirmation of the direction that the world is going, once again implying a short-cutting rather than due-process view on scientific and technological advice. Such statements vary between the softer "ID Cards are an idea whose time has come" to the more emphatic claim that "without regard to Parliament's decision on identity cards, biometric passports collecting iris, finger and face scans are an inevitability".

Implementing organisational or technological change

45. Government clearly wants to do something to fix problems it recognises. However, actually fixing the problem often requires changing the way people do things. Changing behaviour is hard, and you risk the wrath of those people who generally don't like change because it is extra work. So instead, the government proposes technological solutions, which may also mandate organisational change ("because the technology says so").[29] The technological changes also have the benefit of being more visible than organisational changes.

February 2006

APPENDIX 9

Memorandum from LASSeO

1. Background

LASSeO, the Local Authority Smartcard Standards e-Organisation, was created in March 2002 from interested local authorities and partnerships, at the suggestion of the ALCO partnership, to assist the local authority sector by reducing the risks caused by a lack of agreed standards for the public sector.

LASSeO, as its name implies, is concerned with doing this by selecting or developing standards and specifications for the public sector. The organisation's mission is to ensure that the full potential of smartcards is harnessed in the delivery of local authority electronic services for the benefit of UK citizens, by defining and monitoring interoperability standards and frameworks across platforms, issuers, local services, and environments.

LASSeO acts as a smartcard standards body for local government and has excellent links with industry and other standards bodies. As such it is well positioned to be aware of any external contact from the Home Office National ID project.

Like other players outside central Government, we find the whole process highly opaque. We have no direct knowledge of the existence of Chief Scientific Advisors let alone their impact on the Policy making process. Our industry links lead us to believe that levels of skill in this technology are low within government circles.

Throughout the comments below we are assuming that the term Scientific Advisers includes responsibility for technology. In general terms (possibly with the exception of biometrics) the science is determined but the technology involved in deploying it is the case in point here.

[28] House of Commons Home Affairs Committee (2004) *Identity cards.* Report HC130–I Archived at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130.pdf Para 222

[29] Neil Postman (1992) *Technopoly: The surrender of culture to technology.* Vintage Books, New York says "I am constantly amazed at how obediently people accept explanations that begin with the words 'The computer shows . . .' or 'The computer has determined . . . '. It is Technopoly's equivalent of the sentence 'It is God's will', and the effect is roughly the same". Page 115.

2. Summary and Conclusions

As an organisation that aims to support the deployment of smartcards in the public sector, LASSeO is very keen to ensure that whatever arises from the National ID card scheme works well with other public sector card schemes.

The National ID scheme demands attention from the wider public sector because, if it is implemented well, it could provide a very useful fillip to mass card deployment and could significantly change the authentication landscape. However, if not implemented well, it could put back the status of smartcards many years.

In the event, the whole science/technology/advice process and its impact on policy have been opaque. As stated below, it is very difficult to discover an accurate and authoritative position on current thinking about what technology will be deployed and how it will be used.

Presumably the project has been through some kind of gateway process but this remains unclear outside the project. Indeed, the process underway is not known or understood by large parts of the smart card industry and there has been a lack of detailed engagement with some obvious external peer groups. The run-down of the e-GU Smartcard Working Group is a classic case in point. A fairly strong, technically able group that was effectively providing free review of government smartcard activity has been allowed to lapse without any obvious replacement mechanism.

There now appears to be no external scrutiny of the technology being adopted and the quality of the process could be considerably improved by the establishment of an external peer group review. If carefully chosen and properly funded, this would perform the role of critical friends who could become ambassadors for the technology being used within the project.

3. The Detailed Issues are Addressed in Turn Below:

3.1 *Sources and handling of advice*

What impact are departmental Chief Scientific Advisers having on the policy making process?

We suspect very little—this involvement has not been visible at all to those outside Central Government.

What is the role of the Government Chief Scientific Adviser in the policy making process and what impact has he made to date?

Again, this involvement has not been visible at all to those outside Central Government.

Are existing advisory bodies being used in a satisfactory manner?

LASSeO was initially involved in some early discussions around appropriate standards and had some passing input to e-GU support provided to the project. This effort would have been able to be sustained and the input greater had even limited funding been available.

As an influential organisation, we receive frequent questions about this project from other forums and local authorities indicating that other usual channels have not been adequately engaged.

Are Government departments establishing the right balance between maintaining an in-house scientific capability and accessing external advice?

LASSeO believes that there is a general lack of smartcard expertise in central government and, although strenuous efforts seem to have been made, believes that more work is required here. We are not aware of significant attempts to access external advice, outside the initially inexperienced (in smartcard terms) consultancy used within the project.

3.2 *Relationship between scientific advice and policy development*

What mechanisms are in place to ensure that policies are based on available evidence?

The e-GU has advised the Home Office on the ID project but its access to available evidence has been limited by the winding-down of the e-GU Smartcard Working group that existed early in the project development.

This Working Group should have been used as a much needed peer group for external challenge and review but it has been allowed to fall into disuse.

Are departments engaging effectively in horizon scanning activities and how are these influencing policy?

As suggested above, technology specialists and those in the smartcard industry who might expect to be involved have not been engaged in the project.

If this activity is being carried out, it is not visible outside government circles.

Is Government managing scientific advice on cross-departmental issues effectively?

Taking a wider view, the answer is no. Engagement with technology advice on wider cross-public sector issues has been, at best, sporadic.

3.3 *Treatment of risk*

Is risk being analysed in a consistent and appropriate manner across Government?

No comment.

Has the precautionary principle been adequately defined and is it being applied consistently and appropriately across Government?

No comment.

How does the media treatment of risk issues impact on the Government approach?

The media treatment of risk issues has had an undue impact on the Government approach. The amount of "noise" surrounding the project has made it very difficult to engage with. It is very difficult to establish what detailed plans exist or are being developed, what technologies will be selected, how these technologies will be used, etc. This has been a major factor in the lack of engagement from local government, and some degree of scepticism from technologists outside the project.

3.4 *Transparency, communication and public engagement*

Is there sufficient transparency in the process by which scientific advice is incorporated into policy development?

No, the process is very opaque. The ways in which scientific advice is incorporated into policy development remain a mystery to those outside Central Government.

Is publicly-funded research informing policy development being published?

If this is so, information about the process is not easily accessed.

Is scientific advice being communicated effectively to the public?

No. It is difficult to distinguish between scientific advice and hype. There is huge difficulty in accessing authoritative, accurate, information, and being sure that it is up to date. The result of this is a confused situation where public understanding of the science and technology is being led by the news media that tend to dwell on some possible outcomes.

3.5 *Evaluation and follow-up*

Are peer review and other quality assurance mechanisms working well?

As stated above, peer engagement and review outside central government is not working well, if at all. The lack of external review also makes it difficult to believe that internal quality control mechanisms are being properly applied.

What steps are taken to re-evaluate the evidence base after the implementation of policy?

See above.

4. The Author

The author of this response is Chair of the Local Authority Smartcard standards e-Organisation and is an ICT consultant with particular interest in the use of smart cards in the public sector. He is responding on behalf of LASSeO.

February 2006

APPENDIX 10

Memorandum from Peter Tomlinson, Iosis Associates

Executive Summary

The author submits that ID Card policy was developed in relative isolation from technology information and expertise, except for biometrics, and that that isolation continues—but it is believed that tentative new outreach from other Depts has recently started. The author concludes that the following are still not addressed in the project:

— real technical requirements of other Departments of State and of the Local Government area; and

— established government policy on Information Assurance.

However, the author accepts that international standardisation has not provided sufficient underpinning for the ID Card project's vision, and then argues that the necessary expertise and pre-standards documents are available but are being ignored by the project and brushed aside at the standardisation level by vested interests in continental European industry. UK central government is largely seen as not assisting standardisation, and is handicapped by procurement and internal departmental rules when it tries to form technology partnerships with the private sector.

Submission

1. The Committee states that it is charged with examining the "expenditure, policy and administration of the Office of Science and Technology and its associated public bodies"[30].

2. The Home Office ID Card project is technically an Information and Communications Technology (ICT) project. Much of the design and implementation of such a project should therefore be subject to engineering discipline.

3. In those areas of ICT where industry, commerce and the public sector discuss the technology of secure methods and participate in the development of international standards, including topics in the use of smart cards in the hands of citizens, the OST is not visible and does not participate.

4. The POST Report 200 on Government IT Projects[31] is the result of a study of IT, not of ICT. IT in government is typically a configuration of servers, secure internal networks, and client terminals systems. ICT:

— involves a much wider network of often insecure communications channels (in many cases this will include communication across the public internet); and

— incorporates stand-alone terminal systems that may well connect to a variety of servers under the control of many organisations.

5. UK central and local government, and the European Commission, encourage the use of ICT to provide and support services to citizens. For example in the UK:

— Central government departments (eg Revenue and Customs) provide, through the Government Gateway firewall, a growing number of on-line services accessible across the public internet.

— Local Government, encouraged and supported by ODPM, has implemented on its web sites a number of transaction services as well as providing information, and is slowly adopting smart card technology.

— DfT (and its predecessors) has supported an initiative intended to introduce seamless electronic ticketing in public transport, albeit not without some significant difficulties.

[30] Note to editors at end of S&T Committee No 9 Press Notice.
[31] July 2003.

6. ICT has been rolling out since access to the internet became widely available. First to take it up in volume were commercial organisations that could afford the relatively high communications costs, and more recently it is available to most of the UK population[32] and to almost all businesses.

7. Standardisation in ICT has developed apace through two routes:

— the community of internet service providers; and

— formal international standardisation and pre-standardisation bodies.

The two sets of standards and specifications are now seen to clash with each other.

8. Within the formal standards bodies, the UK DTI has long been promoting and supporting the development of one very relevant work area: information security standards. These were first developed for IT and more recently for ICT [1]. However, the DTI has delegated many other areas of standardisation to BSI, and in particular all responsibility for standards related to smart cards. BSI has in turn delegated all responsibility for smart card standards to the bankers via their association APACS[33]. The result is that, apart from some admin and expenses support, there is no DTI involvement in standardisation of secure token technology and associated transaction methods, and the ISO/IEC 17799 User Group[34] is largely concerned with the security of centralised IT systems. It has been left to ODPM to move forward in the understanding of ICT in government (particularly of course in local government), but there is no consistent support for standardisation from that source[35]—and OST has not been visible there, either.

9. Internet technology standardisation is in the hands of an international co-operative of Internet Service Providers and suppliers of the technology that they use. The results are pragmatic, directly informed by practitioners, and contribute greatly to the making of a market in the hardware and software systems used within the internet.

10. The EC has invested considerable sums to aid the understanding, development and demonstration of ICT and in particular of methods using smart card technology. They see the technology as a way for the public sector to improve service delivery at the same time as becoming more efficient. However, for secure transaction technology the EC wanted "solutions" but overall found that the standardisation funding enabled the production of mostly components that do not fit together well. Components from different suppliers, while standards compliant, are too often not interchangeable or interoperable[36] and generally do not contribute to the development of adequately secure services. From the UK, the participation in these programmes has largely been by individuals and SMEs—but we do not have a large scale or coherent smart card or secure transaction system provider industry in this country; it is the French and Germans that dominate, with the Dutch not far behind.

11. Overall, I conclude that OST has not participated in the development of technology for ICT for public sector service delivery to citizens. Thus an important guiding hand for the public sector is missing from this area.

12. The author of this submission was alerted to the S&T Committee's request for submissions by way of an email from the S&T Committee office that was forwarded by the Smartex Group, a group of companies operating (albeit on a commercial basis) a set of Forums where industry, commerce and the public sector can interact on ICT and secure token topics. The email set out specific questions[37] of interest to the Committee. The remainder of this submission addresses those specific questions, but first some introductory statements.

13. In para 10 above is a note that the EC wants "solutions". One has to ask: At what level? I contend that ICT is an enabling technology, not an application level set of solutions. But if developers of ICT components and methods do not understand their actual and potential customers, their component and system level solutions will either fail in the market, or, if (as is the case with most of the UK public sector[38]) the customer is not sufficiently informed, the market will stagger along without fulfilling its potential and the customer (and the end users) will not be satisfied. The technology has to be flexible, particularly so in the case of the UK public sector (see POST Report 200 about changing requirements), and therefore has to be decoupled from the requirements of any particular customer's programme while at the same time generalising from them.

[32] Most of those who do not have internet access at home can now easily find Local Authority internet rooms, terminals in educational institutions, public kiosks, and internet cafes; also mobile phone technology is crossing over to internet services.

[33] APACS is currently recruiting a new head of standards, as their long term holder of that post has moved on to "special projects".

[34] That User Group's Secretariat within DTI is distributing its material on paper by snail mail, instead of using email.

[35] Except in one important respect, the ODPM National Smart Card Project became more of a "learning on the job" project for local govt officers rather than a serious set of specifications and guidelines for the deployment of ICT and citizen service smart cards; support for most of the documents produced has now ceased; the important output is a smart card management system and a data map on one type of smart card—for more details contact Bracknell Forest District Council, or Richard Tyndall richard.tyndall@mouchelparkman.com (Programme Manager).

[36] Interchangeable means that similar components from different suppliers can substitute for each other; interoperable means that a component from one supplier will always work correctly across the network in conjunction with another system, no matter who supplies that other system or its components.

[37] See Annex to this submission.

[38] Acknowledged by Ian Watmore at the May 2005 Sheffield e-Gov Conference.

14. The public sector should work in compliance with international and national standards. Too often UK public sector procurements and operational contracts with ICT content do not require compliance with Information Security standards, or with Quality standards (ISO 9000 series and sector specific derivatives), including not requiring compliance with stated government policy on Information Assurance (see [5] to [12]). That has significant adverse consequences for both service delivery and suppliers—and it indicates that risk (the "Treatment of risk" topic in the No 9 Announcement) is not being handled at all well. A 2005 initiative to set up a Local eGovernment Standards Board has failed to gain funding from ODPM. While all of that is a topic in its own right, it does lead to a more general point that was confirmed by Ian Watmore (then eGU CIO) at the e-Government Conference in Sheffield in May 2005: procurement by the public sector of ICT systems and services is today largely in the hands of people without expertise in this technology area, whereas until the early 1990s public sector purchasers of IT systems generally had the expertise or were required to obtain it from a public sector source. There are some similarities today with the problems that small companies had 25 years ago when trying to purchase or lease reliable photocopiers suited to their real needs.

15. My experience and awareness of industry involvement in the ID Card project is mainly from the point of view of SMEs and individual expert consultants. We have considerable contact with central and local government personnel and programmes, as well as amongst our own network of businesses and individuals. We also have some contact with large IT suppliers and consultancies, but that does not usually result in any exchange of information beyond realising that a number of the larger UK businesses who are or claim to be active in this area have very little expertise in ICT and in particular in the use of secure tokens (usually in the form of smart cards) as vital components in secure systems.

16. *Was there sufficient certainty about the technology when the policy was drawn up?*

17. When the current Govt ID Card policy was introduced, it appeared to be very straightforward:

- ID Cards will be introduced, first on a voluntary basis.
- The cards will be smart cards.
- A new population register and database for citizens (and some others) will be created.
- Citizens (and others) will be registered and entered into the new database, using a new process, before being issued with an ID Card.
- The cards will be useable in transactions with the public sector, in order to verify the identity and, where appropriate, the entitlement, of the person carrying the card.
- Transaction records of card holder activity, as evidenced by use of the ID card to access the verification system, will be kept in a database.

18. If that policy is to be implemented as a single centralised scheme with dedicated terminals and a private network (an intranet in today's technology), then, apart from the biometric methods included in the policy, the core system components follow a now classical secure ICT system architecture:

- Smart cards.
- Registration method used to populate a database and issue cards.
- Database.
- Verification service.
- Communications channels.
- Terminals.
- Security management.

19. The author of this submission is not a biometrics expert, and therefore that technology is not addressed here, although some information received in industry seminars is referred to.

20. That, apart from the biometrics, a centralised scheme such as is outlined above could be implemented at the time that ID Card policy was drawn up, and done so securely, was certain:

- The Mondex project demonstrated by 1995, to the satisfaction of GCHQ, that smart cards in the hands of citizens could be used in a secure manner (in the Mondex case this is for storage and transfer of funds within the money supply).
- Database methods, scalable to global scale, were commercially available.
- The banks have had for some time a secure (but expensive) network of ATMs, and another secure (and global) network for inter-bank money transfers.
- That suitable secure, dedicated terminals could be developed and produced at acceptable cost was demonstrated by commercial interests in the USA (Wave Systems) and by a consortium of bankers and industry in France (a development that led to the FINREAD specifications [2] via EC grants).

21. The difficulty was that such a classical system architecture did not fit even central government requirements. Other departments of state were asked how they would use the ID card in their own transactions with citizens, and soon discovered that no provision was being made for linking their own

systems into the central verification scheme, or for dealing with the legal and constitutional consequences. On that second point, it appears that a patient attending at a Health Centre would be asked for a Health Card (a programme being developed by DoH) and an ID Card: the Health Card would be inserted into one terminal and the ID Card would be inserted into another terminal. The ID Card system would then be responsible for telling the doctor (or receptionist) whether or not the patient is eligible for NHS treatment, whereas the DoH wants their system to make that decision[39].

22. Rephrasing the question:

Was the technology for a network of secure systems, using a secure token in the hands of the citizen and widely deployed secure functions in PCs used as terminals, developed at the time that govt policy was made?

23. Again, biometrics are excluded from the answer.

24. No: the relevant technology was at the modelling stage in the e-Europe Smart Cards 2003 programme,[40] but EC funding stopped in 2003 and industry has not picked up the baton. Other countries, particularly Japan, have made some progress since 2003. The USA has attempted to define secure methods, initially for the CAC[41] programme and more recently as a prelude to the Federal employee and civilian contractors secure access programme,[42] but they have not so far succeeded in developing satisfactory networked methods.[43]

25. A correspondent[44] tells me that, at a 14 February 2006 e-Government Forum in Westminster, Andy Burnham MP (Home Office) said that some detailed decisions about technology are still to be made. Would that this could be done in an open forum.

26. *To what extent did the status of technology influence the Government's policy development?*

From my point of view it is impossible to answer this.

27. *Which sources of evidence were used when the policy was developed?*

I can only answer this in the negative: to my knowledge, none of the people with whom I have been in contact, in both public and private sector, were (except in biometrics and perhaps in OeE's security partner CSIA) consulted by Home Office during policy development prior to mid 2005. That there were meetings at which HO was present and independent experts were also present is not disputed, but these were not HO consultations.

28. *Will performance levels of technology be established far enough in advance?*

29. If the simple architecture set out above is implemented, performance levels (except perhaps for biometrics) are already known from schemes in other countries. In the biometric field, information made available in industry seminars suggests that performance levels are now known, but that only expensive equipment (costing an order of magnitude more than the HO's £750 per terminal to purchase and properly install) will provide adequate performance, and only then when managed and operated by skilled staff.

30. If a true distributed network is required, it will not be possible to re-engineer public administration within the ID Card project timescale, and linking together the systems of the many departments of state, together with local govt, is still an unknown quantity. That is not to say that we could not now plan the architecture of a staged identity management system that could quickly be of use to many public sector bodies.

31. *What mechanisms are in place for feeding ongoing developments in technology into the plans for policy implementation?*

32. Apart from biometrics, none. Encounters with some large systems implementors suggest that the procurement process inhibits such feeding in of developments. Specialist secure systems suppliers who wish to participate in this type of project are all offering proprietary technology, and there is no forum for them to work as a group with Home Office on common interface specifications. International standardisation is not producing specifications directly applicable to the real multi-authority secure transaction methodology requirement of the project, in part because the UK does not fund or organise the necessary participation.

[39] Hot off the press is a 21 February article in *Computer Weekly* reporting a new initiative in linking departmental systems: "A cross-government committee has begun developing a technology roadmap that will allow local authorities to build ID card checks into their websites . . ." http://www.computerweekly.com/Articles/2006/02/21/214300/IDcheckstogoonline.htm

[40] The author of this submission was editor on the modelling project (OSCIE GIF)—see [3].

[41] Common Access Card: US military ID card.

[42] Mandate issued by President Bush in August 2004: Homeland Security Presidential Directive-12 (HSPD-12).

[43] Discussion with USA representative during Plenary Meeting of the MMUSST CEN/ISSS pre-standards Workshop http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/ws-mmust.asp or www.mmusst.org.

[44] Mick Davies, who is associated with the Sheffield e-Gov Centre of Excellence and is Chair of LASSeO (Local Authority Smart card Standards eOrganisation, a voluntary group).

At the UK SME and individual consultant level, HO started in 2004 to attend Working Groups hosted in both public and private sectors, but in general (again I exclude biometrics) the HO attendees are not experienced in secure systems and smart card technology or in the management of technology, and the encounters have been at best barren.

33. For example:

(1) DfT-sponsored Transport Card Forum Working Group 14: HO representatives have attended several meetings. At one meeting a person from the HO's team of consultants from PA was present, and she admitted that there were no smart card specialists in the PA team.

(2) eGU Smart Card Working Group (govt representatives and invited consultants) determined, by the time of its last meeting (Feb 2005), that:

— there was no route for other public sector bodies to feed requirements into HO policy;

— eGU had no money to develop, and no authority to enforce implementation of, a detailed specification for cross-departmental identity management (although later in 2005 eGU did gain some funding, and has worked with ODPM on the Government Connect project[45]).

34. eGU SCWG was to a limited extent a useful peer group mechanism, but it seems that eGU attention moved back to single schemes and systems rather than cross-department collaboration. It should be noted that attendance at SCWG by independent experts and consultancy companies was not funded, yet eGU was clearly in need of expert assistance.

35. *What is the role of international co-operation and advice?*

36. Within the European Commission there appears to have been a disagreement on how far the Commission can mandate features of a smart card ID Card. Legislation gives each Member State the responsibility for the design of any ID Card that they wish to issue, but some argue that the EC can and should mandate the electronic content. In the end the Commission has made no pronouncement, and thus there is no Directive on electronic content (including security).[46]

37. CEN Technical Committee 224 WG15 is developing a European Specification for a Citizen Card—it turns out that this is an ID Card specification. However, the work is dominated by French and German commercial interests and suffers from the general problems of standardisation in this field: too many options, no work on system level security and risk management, the clash between internet specifications and smart card standards, and acceptance of insecure PCs as terminals with no provision to mitigate their insecurity.

38. As noted in para 24, the eESC 2005 programme was not funded, and it did not proceed. It intended to have information security and e-ID (use of secure ID across the internet from home and office) as major topics. However, a small number of the earlier eESC participants are attempting to operate a global e-ID forum.

39. Countries around particularly the northern hemisphere have ID Card programmes, and the USA has its federal programme (para 24), but these appear to be developed in isolation, despite promises of interoperability.

40. *Has the cost of the technology been accurately estimated?*

41. No, not even for the basic central scheme and dedicated terminal architecture—this is primarily because of the biometric technology being under-developed, partly because procurement rules prevent accurate price estimating, and I suggest partly because there is no real scheme design available and no experts employed on costing.

42. The more general networked development, involving alignment of databases across multiple central government departments and with local govt (a core part of general administrative process re-engineering) is, I believe, just now beginning to be discussed between ODPM and eGU. Costing is a long way away.

43. *To what extent has the Government invested in R&D to enhance the understanding of the technology and to further develop the technology itself?*

44. Direct investment: None that I know of (but then I'm not involved in biometrics work).

45. Indirect investment: UK contributes to EC funds from which grants are made to R&D and technology projects. However, EC funds have since 2003 largely moved away from projects relevant to public sector ICT.

[45] Some information can be found at [4], but the major secure development is the enhancement of the Government Gateway to provide secure identity management by means of a PKI.

[46] However, there is a Directive on electronic signature, which mandates use of a smart card as the Secure Signature Creation Device. The current HO ID Card project does not require electronic signature, but other departments may wish to use it as they learn from the experience of other EU countries.

46. Government Connect (ODPM funded [4]) intends to move into e-ID and will have to consider R&D in this area, but it is currently concentrating on secure email for local govt officers and outside organisations with which they work when handling personal information (eg in social services, where I have personal experience of the current use of insecure email).

47. *The author*

The author of this submission is an independent consultant in ICT strategy and secure solution design, with particular interest in smart cards and associated secure terminal equipment. He has contributed to several European pre-standardisation and standardisation projects in this area, and was contracted in 1999–2000 to carry out a technical edit on the UK Government smart cards Modernising Government Framework [12]. He has also been a Director of the ITSO[47] management company, and is currently consulting on a public sector travel concession pass project compliant with the ITSO specification and method. During the 1990s he managed a company providing technical services to the Mondex e-money card project and related banking projects.

February 2006

48. References

1. BS 7799-1 and -2, and more recently their international successors ISO/IEC 17799:2005 and ISO/IEC 27001:2005 (BS 7799-2:2005); also BS 7799-3:2006.

2. www.finread.com, plus continuing work in the Global Platform consortium www.globalplatform.org

3. Global Interoperability Framework (GIF) for Identification, Authentication and electronic Signature (IAS)—see Volume 3 of the Open Smart Card Infrastructure for Europe (OSCIE), available at www.iosis.org/oscie.

4. Government Connect www.govconnect.gov.uk

The following UK policy documents are catalogued at a series of web pages starting at http://www.govtalk.gov.uk/archive/archive.asp?librarydocs=5

5. Security—e-Government Strategy Framework Policy and Guidelines Version 4.0.

6. Assurance—e-Government Strategy Framework Policy and Guidelines Version 2.0.

7. Registration and Authentication—e-Government Strategy Framework Policy and Guidelines Version 3.0.

8. Trust Services—e-Government Strategy Framework Policy and Guidelines Version 3.0.

9. Network Defence—e-Government Strategy Framework Policy and Guidelines Version 2.0.

10. HMG's Minimum Requirements for the Verification of the Identity of Individuals.

11. HMG's Minimum Requirements for the Verification of the Identity of Organisations.

12. Smart Cards Framework: Modernising Government: Framework for Information Age Government: Smart cards.

APPENDIX 11

Memorandum from Intellect

1. Background

(a) Intellect represents 1,000 companies in the Information Technology, Telecommunications and Electronics industries in the UK. Intellect is committed to improving the environment in which our members do business, promoting their interests and providing them with high value services. Our membership spans blue chip multi-nationals through to early stage technology enterprises. Many of our members have been involved in similar card schemes across the world.

(b) This submission has been prepared specifically for the Committee but draws on the views expressed in previous papers written by Intellect. These papers can be found at http://www.intellectuk.org.

[47] Integrated Transport Smart card Organisation, responsible for developing and managing the specification and support services for the DfT-sponsored and mandated electronic ticketing method for public transport www.itso.org.uk

2. Executive Summary

(a) Intellect welcomes the opportunity provided by the Committee to participate in this inquiry.

(b) Intellect believes that its members and the wider UK technology industry (suppliers of cards, security technologies and integration services) have the ability to meet the technological challenges created by the Government's proposals.

(c) Used effectively, technology has the power to redefine the relationship between public services and citizens. It has the power to enable personalised services and reach out to vulnerable groups in the way that traditional services may be unable to. But only when people are put at the heart of public service development, from conception through to implementation and ongoing review, will technology really add value.

(d) Therefore the Government is keen to ensure that it seizes the opportunities that are presenting themselves now, and over the coming years, to transform public services for citizens, business, and frontline workers through effective use of modern technology.

(e) The successful implementation of any programme is dependent on technical and commercial imperatives taking precedence over the political considerations and deadlines imposed on the supplier community. Too often, political concerns have impeded the successful implementation of such projects.

(f) Intellect recognises the challenges presented by the ID Card Programme and calls on the Home Office to ensure that it manages the evolving supplier landscape and any forthcoming procurement process on the basis of openness and partnership, in line with the behaviours outlined in the Intellect IT Supplier Code of Best Practice and consistent with the SRO/SRIE initiative. The personal engagement and leadership of a senior executive from the user business is essential to the Programme's overall success.

3. Introduction

(a) Any kind of change to public service utilizing new or existing technology needs to be properly planned. Although this may seem an obvious statement, transforming public services goes far beyond just technical or organisational change.

(b) Too often large-scale changes in technology have failed to bring about the improvements envisaged because of an over-simplification of the required changes, unrealistic expectations about the pace and speed of delivery and failures in overall project management.

(c) Too often public sector IT projects are cited as "invariably" costing more than planned and delivering little or no discernible benefit. In reality, the projects which grab the headlines are mainly those which focus on introducing changes in the way that people work—both citizens accessing services and the Government employees in providing services; via telephone, the internet and interactive television. In such projects, IT is just one component. An understanding of wider business change is often overlooked or, perhaps more worryingly, not understood.

(d) Pure IT projects are delivered every day—upgrading computers, networks and communications to do the same job as old equipment but do it faster, better and cheaper. Such projects do encounter difficulties but no more than other complex pieces of work in construction, engineering and hi-tech development such as the London Eye, Millennium Stadium, Millennium Bridge, Jubilee Line Extension or the West Coast Mainline—projects which in the longer-term have come to be considered successful. In comparison, projects of a similar scale are delivered successfully by the IT industry on a regular basis.

(e) Indeed such successes have already been realised, and possibly taken for granted, in the public sector—new passport applications processed in four days, Car Tax paid without having to visit a Post Office and Land Registry searches done in days rather than weeks.

(f) Not enough consideration is given to the impact of new technology on employees, users and members of the public. Any IT-enabled business change project requires, where applicable, consultation with the citizens, preparation for staff (eg from CIOs and respective Heads of Personnel in the case of Shared Services), analysis of the impact on service deployment and pre-emptive action to deal with any expected increases in demand.

(g) Overcoming cultural barriers and silo mentalities across the public sector will therefore be critical. IT has often worked in isolation from the business and other back office functions. If the nature of change is to be better understood, both as a profession and as a solution IT needs to work collaboratively within and across organisations to support better-integrated solutions that will address the increasingly joined-up nature of government.

4. General Comments on the National ID Card Scheme

(a) Intellect believes that the National ID Card should not be seen as an isolated IT project but rather a wider IT-enabled business change programme. Such an understanding is a crucial part of implementing a solution where technology is but one aspect of a much wider modernisation programme. Only through achieving a comprehensive understanding of the industry, its capacity and capabilities will the Government be in a position to develop an ID Cards Scheme capable of delivering on its promises to citizens.

(b) It is important to recognise that although the ID Card debate has focused primarily on biometrics so far, there is more to ID Cards and identity management. ID Cards and identity management issues also include data management, security, audit, authorisation/authentication, storage, data retrieval and potentially data sharing with other Departments/Agencies. These issues are likely to present greater long-term challenges.

(c) It is industry's belief that the Government's proposed ID Cards Scheme should be built on technology and business processes that have been proven in existing implementations around the world. Most European countries have ID Card programmes and some are moving ahead with systems that offer real advances in citizen confidence and convenience, and include security and other multi-functional capabilities. For the citizen, as consumer of public services, such schemes offer more convenient access; for the citizen as taxpayer, the scheme offers public services delivered with increased operational efficiency.

(d) The industry has experience of delivering these programmes successfully and Intellect urges all relevant parties to engage with the supplier community to better understand how best practice can be accessed and how real citizen benefits can be demonstrated. It is imperative that the Government selects a solution that is proven to work, and not one that is selected solely on the grounds of cost.

(e) Moreover, this Programme represents an excellent opportunity for the Government to encourage significant collaboration between suppliers, particularly regarding linkages between service and IT architecture.

(f) This procurement is a significant undertaking. In order to proceed effectively the Government must have:

- Strong political and public support.
- Confidence in the equipment.
- Confidence in the process (with no scope creep).
- Ringfenced funding.
- Accountability and audit of the operation.
- Testing—technical, procedural and physical penetration testing.
- Accreditation—regarding documentation, risk assessment, operating procedures, and safety case.

5. Specific Comments to Committee Questions

(a) *Sources and handling of advice*

(i) With particular reference to the ID Cards Scheme, Intellect has not had any engagement with the Government Chief Scientific Adviser. The Programme states that it intends to encourage innovation. There needs to be a process that enables innovative specialist suppliers to present to identified primes for each package and to the client, so they are aware of the benefits of small suppliers. This needs to be supported by project management arrangements to ensure specialist subcontractors have access to the client during delivery.

(ii) Therefore, Intellect believes that the Government needs to do more to engage with sources of external advice at the earliest stages of Government projects. This takes on greater significance as more and more policy initiatives have significant technological ramifications. Later in this submission Intellect provides details on its Concept Viability Service. This is an initiative which has been used by a number of Government departments and agencies since its inception in late 2003.

(iii) However, Intellect believes that Ministers, MPs, Special Advisers and key officials should engage with the private sector has soon as any policy is formulated in order to better understand the market's capacity and capability to deliver any given solution.

(b) *Relationship between scientific advice and policy development*

(i) Intellect welcomes the basic approach taken by the Home Office during its period of consultation and deliberation. Officials have given a number of presentations to suppliers and this has enabled the development of an open dialogue between Government and industry regarding the technical issues surrounding the implementation of an ID Card.

(ii) This may be seen as a horizon scanning activity, however it is not clear at present how this activity will influence the outcome or specification for the ID Card Programme. It is assumed that evidence is made available as an input to develop policy, and that evidence here refers to market, service or technology capabilities. Ideally, we would like to see a final Statement of Requirements prior to commencement of procurement, and also to know what elements of a Statement of Requirements have been introduced or amended in response to this market sounding activity.

(c) *Treatment of risk*

(i) Public trust and confidence is fundamental to success of any project, but especially to one of such importance and sensitivity. To succeed, the Government proposals must address the twin perspectives of citizens (citizen/consumer and citizen/taxpayer) and focus particularly on citizen-centric needs, including, for example:

- the value of the card to citizens—the benefits need to be tangible and compelling;
- the trust of citizens in government—this must be earned and safeguarded;
- the security of personal data—the integrity of the programme depends on this; and
- Government intentions—these must be transparent and visible in order to overcome negative perceptions.

(ii) In combination, these factors require that the Government's business proposition is substantially citizen-focused: an ID Card will have to deliver rapid and compelling benefits to citizens to shift negative perceptions and establish the foundations for long term adoption.

(iii) Therefore, system requirements that are inadequately explained and thought through in the procurement specification or changed during the process create an unacceptable burden, especially for smaller suppliers. This could be exacerbated by the lack of clear end-to-end accountability.

(iv) Moreover, with a programme of this scale and duration, requirements may change significantly over time eg involving more departments or commercial organisations. The change process can create major issues unless it is well managed by both the supplier and contacting authority.

(v) Accepted best practice in procurement, as documented by OGC, recognises that there needs to be effective risk allocation, whereby each risk is allocated to the party best able to manage it. Ill-considered wholesale transfer of risk to the supplier will very likely include risk that the supplier is less able to manage than the customer. It is in the customer's best interest that risk transferred to the supplier should be manageable by the supplier and proportionate to the scope of the project being undertaken.

(d) *Transparency, communication and public engagement*

With regards to the ID Cards Programme it is unclear, so far, how and what advice regarding the technological and scientific capabilities have been incorporated into the specification. In some respects this is understandable, early notification of specifications and costs which are then subject to significant change due to political considerations create uncertainty among the supplier community. This is especially true for programmes which carry significant reputational risk.

(e) *Evaluation and follow-up*

Intellect's Concept Viability Service does play a part in fulfilling this function, however Intellect believes that even if it is at the expense of meeting politically-inspired deadlines, commercial and technical considerations must take precedence if the evidence suggests that further consultation with the industry is required.

6. Concluding Comments

The reliable delivery of big projects reflects some of the higher-profile difficulties that Government (and the community) have experienced in the past years. Intellect believes that the collaborative efforts of Government and Industry through such bodies as the Senior IT Forum have gone some way to addressing this area of concern. However, each new major project will have its own challenges, and will require experienced teams from Government and Industry, who take full account of all the learning and guidance that have arisen from experience of this issue.

February 2006

Annex 1

Intellect Concept Viability Service

(a) One of the key challenges facing the public sector is how to transform policy ideas into desired outcomes, particularly when this involves IT-enabled business change. Concepts that appear straightforward on paper can be extremely difficult to execute, especially when the technology is new or emerging, or when transaction volumes are very high.

(b) In recognition of this difficulty, one of the six actions agreed by the Cabinet in December 2002 was that "no government initiative (including legislation) dependent on new IT would be announced before analysis of risks and implementation options has been undertaken." This action was clearly designed to help senior public sector decision makers assess the key factors and risks involved in the delivery of their proposed IT-enabled programmes and projects.

(c) The Office of Government Commerce recommends early involvement of suppliers. Suppliers welcome the opportunity to meet with prospective customers and advise them on the "do-ability" of their idea and to discuss key issues related to potential solutions. This allows suppliers to show the client how the market can meet their need, provides early visibility of key risks and issues, and gives suppliers the opportunity to manage expectations of what the market can and cannot contribute to the proposed programme. Intellect fully endorses this approach and offers a Concept Viability service to public sector clients to help them consult the market.

(d) Through its Concept Viability service Intellect is inviting public sector clients to take market soundings to test the practicability of their ideas at the earliest possible stage. Within the Gateway process this would be before Gate 1 (and may even be before Gate 0), and before any public commitment (political, financial or "go live" date) has been made. In essence, the earlier the concept is tested, the better; clients will gain greater understanding of the achievability of their ideas and high-risk proposals can be modified or abandoned before any substantial investment has been made.

(e) Clients with business needs that require either a large-scale commitment or demanding solution would approach Intellect to test the viability of the concept. As the leading representative body for the ICT industry with approximately 1,000 member companies, Intellect is well placed to draw on the expertise clients need. Intellect is also technology-neutral and so will be able to draw on a range of companies providing fundamentally different solutions, thereby enhancing the variety of options and perspectives available to the client. If the client suggests the involvement of specific companies outside its membership, Intellect will be pleased to include them in the process.

(f) This service is intended to assist the development of a more comprehensive assessment of projects at their earliest stages. To this end, the assessment proposed in this document should not be viewed in isolation, but rather as part of a wider consultation undertaken by the client (ie this will not replace work which the client undertakes on proof of concept or feasibility, but rather seeks to inform it).

(g) Intellect would be happy to provide details of the workshops it has run to date with Government departments.

Annex 2

Intellect IT Supplier Code of Best Practice

(a) The Intellect IT Supplier Code of Best Practice outlines the standards of professionalism and behaviour that should be most likely to improve the success rate of IT-enabled projects and programmes. The Code was developed following discussions with key Government customers and a wide variety of Suppliers. It consists of Ten Commitments, all of which are focused on actions by the Supplier, although some call for corresponding behaviours by the Customer if the full benefits are to be realised.

(b) The emphasis is on establishing an open and effective relationship as a platform for success, both during the acquisition phase and throughout delivery. It represents a major commitment by the industry towards a more mature procurement environment. The Code gets to the heart of some of the key issues that have inhibited success in the past and it sets out the practical improvements that should be most likely to yield real benefit.

(c) The Commitments outlined within the Code provide a basis for partnership, but reciprocal action from customers is also required and should be encouraged.

APPENDIX 12

Memorandum from Dr Itiel Dror, School of Psychology, University of Southampton

THE GOVERNMENT'S USE OF ADVICE AND EVIDENCE IN DEVELOPING POLICY: TECHNOLOGIES SUPPORTING THE GOVERNMENT'S PROPOSALS FOR IDENTITY CARDS

EXECUTIVE SUMMARY

Technological and scientific advances rarely initiate governmental policy; more often policies arise from political vision, public pressure, circumstances, and so forth. Thus "evidential based" is often obtained and used after political, personal, and psychological commitment, and thus its impact on policy development is limited. There are difficulties and challenges in obtaining good, independent, and objective advice, especially within the time scale of policy development. This is due in part to the nature of research, finding people who are not stake holders or affected by the policy (directly or indirectly), and dealing with long-term predictions that relate to the policy. Technologies and policy do not exist in a vacuum and cannot be examined in isolation; they need to be considered within a wider context, how they can be integrated and work with humans (including people with disability), their social and ethical implications, and so forth. Identification cards and use of biometric technology is a par excellence example of such issues.

1. The Government's proposals for identity cards raise difficult questions concerning technological feasibility, validity and costs as well as wider social implications, all of which shape outcomes in terms of costs-benefits. Also, this is a very large scale long-term project in terms of initial investment, running, constant upgrading and adjustment to new emerging technologies and needs. Thus, just to mention three out of many salient issues:

(i) Should the identify cards be based from the beginning on cutting-edge technologies, with multiple biometric measures and imbedded chips, or should more conventional cards be used in line with the experience of other countries?

(ii) Should the identify cards be initially used only for security purposes or should they serve as a basis for expanding uses, such as national and local licenses and record keeping, including driving licenses, taxation and medical records—on the basis of a national identity number system?

(iii) How much to invest to make the cards as proof as possible against fraudulent acquisition at time of initial distribution and then against general falsification? Being clear from the beginning that making them more secure will require more complex and expensive technologies and measures, and that no mass-used identity card can be completely immune to theft and falsification.

2. This short memo addresses the issue of evidence base for making decisions on these and related issues, leaving out consideration of other issues such as administrative processes for supplying the cards, possible integration into European Union identity cards, and a multitude of political, legal and ethical/value issues.

3. In writing this memo comparable experiences with large scale technology-intense projects have been taken into account, as well as personal work of the author in major innovative weapons systems and in forensic technologies and their uses, especially from a cognitive sciences perspective.

4. A fundamental dilemma must be recognised. Unavoidably, many relevant technologies have to be developed after a decision in principle is taken on introducing identity cards and their main initial design. Thus, the decision is in part a "gamble" based on guesstimating, as much of the needed evidence is not ready on the shelves but has to be developed after the initial decision is taken. This is the case because many salient questions can be specified only on the basis of an initial design and after large funds for producing relevant evidence becomes available. Furthermore, most often the time scale of research is much slower than that of policy development.

5. However, taking decisions on the identify card in the absence of much of the needed evidence is risky, and puts much of the evidence production into a "tunnel vision" with evidence casting doubt on the initial decision being unwelcome, to put it mildly. This not only leads to the lack of objective and reliable evidence that can really be used for policy development, but the optimistic nature of such assessments downplays (if not totally overlooks) vulnerabilities and potential pitfalls.

6. Therefore, maximum efforts to collect and process objective and independent assessment on the proposed identity cards to produce adequate evidence for making a preliminary decision on the identity card are recommended and missing. This evidence should mainly include the feasibility of the policy and its effectiveness. It should also include cost estimates, evaluation of public reaction, and wider social and ethical implications. Field experiments such as with preliminary versions of alternative identity card dummy examples may also be essential. Such steps are all the more important because once an initial design is approved changing it becomes difficult.

7. In any case, the initial design should be "robust" in the sense of permitting adjustment to emerging new evidence. Given the lack of evidential based initial decision, it might be advisable to include into the initial decision a formal proviso that after five years the initial design will be reconsidered totally on the basis of available new experience and evidence with the design to be revised and even discarded as far as may be

justified. This five year review and relevant evaluation studies should be entrusted to independent bodies not having a vested economic, political, or bureaucratic interest in sticking with the ID scheme in general, or with the specific initial design.

8. In other words, introduction of the identity card, even if it were initially based on the best and objective evidence available at that time, should be regarded as a "proof of concept" with a steep learning curve, provisional until re-evaluated and re-approved with less or more radical changes.

9. In tandem with the initial decision, large scale funds should be made available for basic research and technology development essential for more advanced phases of identity card design and production. Doing so will assure that salient evidence becomes available in time when the initial design is re-evaluated so as to reduce lag of identity cards after experience and knowledge and minimise the need for further "gambling" and enforced retirement of identity cards made prematurely obsolete because of too early "freezing" of designs not based on evidence that could have been available.

10. Introduction and usage of identity cards is a critical choice for generations to come. From the onset proper objective and independent research should have been carried out so as to advise and shape the development of the policy. However, policies are rarely initiated and motivated by evidence; they result from political vision, public pressure, circumstances, and so forth. Hence, "evidential based" knowledge is almost always obtained and used after political, personal, and psychological commitment. Therefore, advice is too often obtained only as far as it can support the existing and on-going initiative. Thus, its input in shaping policy is relatively limited.

11. Furthermore, it is imperative to obtain advice and "evidential base" from capable, independent, and objective researchers who do not have personal, political and economical interest in the policy. Whatever the quality of the initial design, emerging technologies together with experience with uses of the identity card, including falsifications, will require periodic redesign with the help of new technologies. Therefore it is recommended to accompany introduction of identity cards with constant research and development and evaluation by independent bodies.

12. It is cost-effective to increase the utilisation of identity cards for additional purposes, such as licensing and record keeping. This raises issues of privacy on the one hand, while permitting improvement in services to citizens on the other. To provide options for such expanded uses without deciding on them prematurely, the basic design of the identity card system should include salient features such as a national identity number to be given at birth. Here, again, evidence on relevant experiences in other countries should be collected together with small scale field experiments to develop most user-friendly and publicly acceptable processes. This should be done to provide options for the future even if no present decisions on expanded utilisation of identity card numbers are taken.

13. Budgets for introducing identity cards should be accompanied with appropriate budgets for result evaluation and technology improvement. Such budgets should in part be "tactical", applied to upgrade the design as initially adopted. But in part it should be "strategic" and basic, to reconsider the basic initial design. The "strategic" budget and its allocation should be supervised by an independent body.

14. It is difficult to estimate in advance the amount of resources that should be allocated to production of new relevant knowledge and technologies, both basic and applied. However, as an initial conjecture based on experience with other large-scale Research, Development and Engineering endeavours, it is recommended that about one to three per cent of the costs of the identity card project as a whole is a very cost-effective long-term investment in relevant evidence production. This includes also social technologies, such as on making the project as a whole very user-friendly (to all members of the public, including elderly people and those with disabilities) without sacrificing its security goals.

15. To move ahead in the aforementioned directions it is suggested to appoint a Chief Scientist for the identity card authority, making sure a highly qualified and independent person with a scientific background fulfils this position. He should be supported by an independent science and technology advisory group. This Chief Scientist should participate in all high level decision making forums and be entitled to appeal against decisions which in his view contradict available evidence to the Minister in charge, perhaps with access to an appropriate Parliamentary Committee.

16. To the best of the partial knowledge of the author, only limited steps in the directions recommended above have been taken.

February 2006

APPENDIX 13

Memorandum from The ALCO Group Limited

THE TECHNOLOGIES SUPPORTING THE GOVERNMENT'S PROPOSALS FOR IDENTITY CARDS

SUMMARY

1. The principal issues this project raises are:
   — Lack of co-ordination with other departments and Government policies.
   — Unwillingness to adapt in any way from the path chosen at the outset.
   — Lack of effective oversight to effect change.
2. The result is:
   — A scheme which make little use of existing infrastructure and is consequently extremely costly to the point of impracticality.
   — A scheme which does not meet other Department's needs.
   — A scheme which is not in line with Government initiatives such as Joined-up Government and Transformational Government.
   — A scheme which has lost the hearts and minds of the press and public which will lead to at best apathy and at worst antagonism with low take-up and usage.
   — A scheme which does not benefit the citizen.

DETAIL

Our Credentials

3. ALCO is a consultancy specialising in the support of ICT based systems and services in the public sector. In particular, most of our work covers the planning for and development of smartcard systems, with and without biometric security support. Much of our work is early stage work where we carry out feasibility studies, strategic analysis and business cases. In addition, we are heavily involved in analysing and supporting user requirements, including the requirements for accessibility and inclusivity.

4. We believe that our extensive experience in this subject area, knowledge of the development and design of the proposed ID card system, experience with user issues, and knowledge of government requirements, puts us in a good position to make value-judged criticism.

Our Concerns

5. We are concerned about a number of issues surrounding the proposed ID card, centred around the relevant Home Office staff being intransigent in their views and not taking on board the comments, requirements and criticisms of others. The result will be a product unwanted and not meeting the requirements of other Government Departments, while losing the confidence and support of both the press and public.

6. Exacerbating the above issues is the lack of oversight of the project by external bodies. The eGU and the OGC have had ample evidence of concern voiced by others but have had no success in persuading the Home Office to modify its design.

7. This will be a major project once it goes forward to implementation. To date the Government's track record is not good in delivering major technology projects on time and within budget. If the Home Office continues to ignore the valid voices of concern voiced at this stage, when the project moves into its implementation phase, it will break all records for being the most costly disaster for such projects ever.

8. As a technologist and a strong and knowledgeable supporter of biometrics, I have to say the plans for the use of biometrics are crazy. No biometric is 100% perfect and this has to be built into the system design. The use of three biometrics to try to hide or account for the problem is not the right way forward. What it will do is tarnish forever the value of biometrics in the public's eye. In addition, no-one will support the use of three biometrics for authentication, for example in a bank, while the use of just one biometric will be queried on the basis that if registration requires three, how can it be good enough to use just one for authentication?

9. We have concerns about the databases being accessed and linked as part of the registration and vetting process. While such use may be valid, we have had no corroboration from the Information Commissioner based upon the planned actual methodologies and usage. This issue highlights another concern which is about communication, which is something the Home Office ID team does not do in the course of its work.

If the ID card team would communicate and keep relevant parties informed, some of our concerns may be allayed, while valid discussions may be started that could lead to acceptance of a requirement for changes on the part of the ID Card design and proposed implementation.

Points of Detail

10. In terms of specific points of detail, the following are highlighted:

11. *Price:* The very high indicated cost of the scheme and corresponding consumer price suggested is considered to be unrealistic and an indicator that the Home Office is unwilling to make use of existing infrastructures such as the Government Gateway. We believe the decision to create a completely new infrastructure to be wrong.

12. *Biometrics:* Biometrics are to be used to enable de-duplication of citizen databases and remove fraudulent aliases. The Home Office has noted that biometrics are not perfect and that different people have more or less success using different types of biometrics. As a result, the Home Office is planning to use three different types of biometric in its registration process. This is clearly not practical in day to day use with the result that biometrics will not be used for validation, and will be used solely for registration. This is a highly expensive approach to take, especially where the benefit is only to the state and not the citizen; and yet, the citizen is being asked to foot the bill.

13. *Stand-alone Nature:* It is understood that the proposed ID card is a stand-alone entity that supports the validation of a cardholder's identity, and that is all it does. The implications of this is that the ID card will achieve its purpose in a manned environment only, since what it will not do is generate an electronic credential (digital signature) allowing it to act as a validator of identity in an ICT environment, that is, support the provision of online services provided by other Government Departments. This flies in the face of government's move towards delivering all services electronically to citizens. It also means that the ODPM's Government Connect project has to follow a parallel track to the ID card which is both wasteful on cost and will be confusing for citizens.

14. *Smartcard Interface Technology:* The smartcard marketplace is in a state of flux from the point of view of interface technology. Historically contact interfaces have been used and the finance sector uses them almost exclusively, as demonstrated by the new Chip and PIN credit and debit cards. The result is a very large infrastructure in place supporting contact card technology. However, the fast developing transport ticketing sector is using contactless interface technology, as demonstrated by the TfL London Oyster scheme. As a result there is a move towards contactless technology in both the public and private sectors. In addition, the use of a contactless interface technology greatly assists accessibility for many with special needs. Even the finance sector is starting to trial contactless payment cards. On the timescale of the ID card, 2008–13, it is apparent that the world will move to contactless technology. Yet the ID card seems entrenched in contact technology. Again, it is a question of listening and learning, something the Home Office team seem unwilling to do.

February 2006

APPENDIX 14

Memorandum from the National Physical Laboratory[48]

CASE STUDY 1: THE TECHNOLOGIES SUPPORTING THE GOVERNMENT'S PROPOSAL FOR IDENTITY CARDS

Sources and handling of advice

The Home Office, DVLA and the UK Passport Service contracted NPL and BT jointly to carry out a feasibility study of the use of biometric systems for personal identification. This review examined known scientific and other objective performance data of biometric systems, for example the benchmark performance used by suppliers of such systems. The conclusion of this study was that biometric systems could offer a viable methodology for identification, but highlighted a number of technical issues that would need to be addressed.

[48] NPL is the United Kingdom's national standards laboratory, an internationally respected and independent centre of excellence for R&D, and knowledge transfer in measurement and materials science. It operates as a GOCO: Government Owned, Contractor Operated organisation. The government owner is the Department of Trade and Industry, and the contractor operator is NPL Management Ltd, a wholly owned subsidiary of Serco Group plc. More information about NPL can be found on our website: www.npl.co.uk

Relationship between scientific advice and policy development

NPL is now under contract to the Home Office to provide expert advice on performance evaluation of biometric systems being considered for ID cards. This is typically four man days a month at present. There are additional external expert advisors from other organisations, advising on performance and usability issues. This advice is being used to support the development of testing during procurement, build and roll out of biometric systems for ID cards. The Home Office is not using experts from biometric suppliers for this advice, because of the conflict of interest this would involve.

NPL has seen some evidence that the Home Office is engaging in horizon scanning activities with other government departments.

The cross-departmental government Biometrics Working Group (BWG) o has been in existence for some years, provides a mechanism for sharing advice on biometrics across government; the group. The BWG has been effective where it is active. Tony Mansfield of NPL is a member of this working group. It comes under the Communication Electronics Security Group of GCHQ.

Treatment of risk

In our opinion risk is being appropriately considered, and assessments of risks used to choose between different options.

There has been a great deal of media interest in ID cards, much of it hostile. In our opinion the government has been cautious in its approach to this debate with the media.

Transparency, communication and public engagement

The report of the feasibility study carried out by NPL and BT has been published and widely quoted in the media. It is our understanding that some details of the testing which will be used to support procurement, will also be published by the Home Office.

NPL has not been discouraged by the Home Office to respond to technical enquiries from the media concerning biometrics and ID cards. We have always restricted our responses to technical matters for which we have expertise. The media has often been selective in quoting our responses, using only those that support the thrust of their story.

Evaluation and follow-up

A Biometrics Advisory Group, chaired by the government's Chief Scientific Advisor, Sir David King, has been established to review the work on the biometrics element of ID cards. The membership of the group is at a senior level, and does not include anyone from, or contracted to the ID card programme.

The extended programme of testing planned for procurement build and rollout will require those running the systems to collect data to provide evidence for the assessment of system performance.

February 2006

APPENDIX 15

Supplementary evidence from the Government

1. In early 2003, as part of the initial feasibility analysis behind the decision to introduce an Identity Cards Scheme, an assessment was facilitated by the Office of Government Commerce to assess its likely technical elements. This exercise included representatives from the Home Office, UK Passport Service, the Driver, Vehicle & Licensing Agency (DVLA), the Office of the e-Envoy, the Office of Government Commerce, the Department of Transport, the National Physical Laboratory as well as external consultants from Fujitsu.

Since that time, a substantial amount of work has been undertaken on the business and technical assumption behind how the Scheme might be delivered.

Ten major technical components to deliver a card scheme were identified at the time. These are listed in Annex A (not printed) as drafted in the report produced at the time. These components included biometric and smartcard technologies. The conclusions reached and agreed by all participants on these two components as reported to Home Office Ministers is reproduced at Annex B (not printed). As these extracts formed part of documents that formed direct policy advice to Ministers, I would be grateful if you could treat them in confidence.

The assessment of these technologies was assisted by previous studies and included analysis produced by the National Physical Laboratory in their report "Feasibility Study on Use of Biometrics in an Entitlement Scheme" and expertise from the Department of Transport in the field of smartcard technology. This

document, including a recommendation to conduct a biometric enrolment trial of 10,000 people was the reflected in subsequent papers as the policy came up for collective discussion, such as at meetings of the DA Committee.

However, the key conclusion of this assessment was that, while certain risks existed around the technical solution for a proposed Scheme, the risks around changes to business processes were greater and this was highlighted to Ministers along with the technical assessments derived from the exercise.

Furthermore, as planning for the Identity Cards Scheme has progressed; the Identity Cards Programme has taken steps to develop its understanding of the risks in these areas as well as implementing the recommendations contained in the assessment through:

- Conducting a biometric enrolment trial with 10,000 participants in line with NPL recommendations
- Employing internal and external advisors to develop the Programme's understanding of biometrics and smartcards further
- Establishing the Biometric Experts Group and Biometric Assurance Group to ensure up-to-date, relevant and accurate advice is considered
- Conducting market sounding exercises to understanding the opinion of companies in the technology sector—such as a smartcard durability survey, which is included at Annex C (not printed).

2. A report on the pilot system for the e-Borders/IRIS project (STP final report) trial report is included at Annex D (not printed). This summarises the deployment of the pilot system and enrolment of approximately 900 individuals.

Since the UKPS Facial Recognition system (utilising 23,000 photos from STOP file entries) has been in operation as a proof of concept, the system has helped to find 432 matching photographs. This confirms that Facial Recognition is an effective tool in the detection and possible prevention of fraud.

The Identity and Passport Service and, formerly, the UK Passport Service have been performing further tests of facial recognition systems. These tests concluded in March 2006 and showed that for 1-to-many face recognition, accuracy rates in the region of 90% can be expected (when using ICAO/ISO compliant search images and given that the top 20 ranked candidate images from each search are checked). The facial recognition database size being used for these tests is in the region of 25,000 images.

Information from other biometric programmes and biometric testing initiatives is fed into the ID Cards Programme through the Biometrics Experts Group, whose members work with a number of these programmes, through the Home Office biometric practitioners' group "Goldfinger" which has representatives from eBorders, the FCO and others and through members of the ID Cards team having a role in the governance of other projects, e.g. the UKPS facial recognition testing project.

3. The decision to use multiple biometrics was made after investigation into biometric technologies which resulted in recommendations which were presented to the programme board in early 2005 and to the Home Office Science and Technology Reference Group, a panel of independent scientific advisors chaired by the permanent secretary.

Developing on previous analysis of biometric technologies, this work looked at the available biometric technologies and investigated what the available scientific evidence had established with regard to their ability to identify individuals and the weight which could be attached to that scientific evidence. It also took into account the merits of including certain biometric technologies, such as facial recognition, for reasons of conforming to international regulations. As a result of this work, the recommendations were that face, fingerprint and iris biometrics should be used.

As mentioned in oral evidence, the factors behind this decision were primarily accessibility to the Scheme for the widest number of people possible, improved performance and the impact of international regulations.

4. In considering the likely performance of biometrics as part of the National Identity Scheme, it is important to note that biometrics checks form one part of enrolment and verification processes. The success of these procedures will not rest solely on biometrics as other more traditional processes and checks of identity will also be employed and indeed, improved on in comparison to what is in place today—through the development of electronic checks against other databases to verify identity information provided by applicants for identity documents, for example.

Nevertheless, the Identity and Passport Service does recognise that biometric checks will need to perform at a high level in order to facilitate efficient verification and secure enrolment. We are using evidence from existing biometric schemes and from biometric test programmes to inform our procurement process, to ensure we get value for money and to enable us to set challenging requirements to the market. We have examined the evidence on matching performance achievable from different biometrics and have found that such performance would be consistent with our requirements.

For face, the failure to acquire rate should be close to zero. The verification rate for face is about 90% with a false accept rate of 1% (FRVT-2002 overview and summary). This report is available at Annex E (not printed).

For finger, the failure to acquire will be 0.5–1% depending on enrolment conditions (UK National Physical Laboratory, report available at Annex F (not printed), validated by the biometric expert group. A false match rate of about 1.3E-10 and a false non match rate of about 0.01 can be achieved. These figures are based on research by the US National Institute of Standards & Technology (NIST IR7110, available at Annex G (not printed)) and make assumptions about the improvements that would result from going from 2 to 4 or more fingers for searching. Those assumptions are based in the improvements found in verification tests more recently—for example, in further research by US NIST (NIST IR7123, available at Annex H (not printed)).

For iris, the failure to acquire rate is approximately 0.5%, when it is assumed that one iris sufficient. This is based on the ITIRT final report for US Department of Homeland Security (available at Annex I (not printed)). Schipol airport trial results indicate 5% false non-match rate and the UAE iris system indicates a false match rate, at the same decision threshold, of approximately 5E-12 although the data were not collected under the same conditions so caution should be used in interpreting these figures.

Note that for fingerprint and iris, threshold settings consistent with a large scale identification application have been assumed, whereas for face 1:1 verification has been assumed.

5. Internal health checks referred to in oral evidence to the Committee are applied to different elements of the programme at times that are important to the development of that individual element of the programme. Thus, they would not be seen as reoccurring quarterly or monthly checks.

However, while these checks may be varied in subject matter, they will be assured thorugh a uniform process. An Identity and Passport Service Internal Review is lead by the Head of Standards and Practices. Two to three additional review team members are drawn from technology and operations divisions, who are independent from the specific project teams. Such reviews follow OGC guidelines depending on the stage the project has reached as a whole.

Furthermore, it should be noted that this process takes place in addition to other review processes such as the scrutiny applied by the Independent Assurance Panel and the OGC's Gateway review process as well as other internal assurance processes within the Programme, such as the Programme's Design Authority and regular risk and issue reviews for example.

6. Advice provided by the Office for Government Commerce is gained from their experience in monitoring and assuring projects and programmes across Government as well as from the experience gained from reviews conducted by the National Audit Office. This experience is then distilled into analysis to assist project and programme managers to improve the quality of projects across government.

Hence, based on this experience, OGC have recommended an incremental approach to programme and project implementation supports project success and have illustrated this in lengthy analytical documents such as "Successful IT: Modernising Government in Action", in which "modular and incremental development" is dealt with at length under Section 5 and Annex E of that document.

In addition, such advice has been reiterated in shorter reference documents such as the pamphlet "*Why IT Projects Fail*" where it advices against sweeping into a single project—"all good ideas—all deliverables in one chunk"

Furthermore, the British Computer Society report "*The Challenge of Complex IT Projects*" states "There is overwhelming evidence that incremental developments are much less risky than big-bang projects" (p.41)

Indeed, these documents also validate the initial findings of the OGC red/blue exercise and the oral evidence provided to the Committee that the key risk lies primarily in the business change that surrounds the implementation of technology rather than just in the implementation of technology itself.

These documents mentioned in this reply can be found at:
"Successful IT" (http://www.ogc.gov.uk/embedded—object.asp?docid = 1005071)
"Why IT Project Fail" (http://www.ogc.gov.uk/embedded—object.asp?docid = 1004824)
"The Challenge of Complex IT Projects" (http://www.bcs.org/upload/pdf/complexity.pdf)

7. The current best estimate of the volume of transactions across both private and public stakeholders is 771m per annum. These estimated volumes, based on stakeholder benefits cases and programme estimates, cover verification, identification, authentication and information provision services. This figure is larger than the estimate previously published as part of the procurement process because of the progress made in understanding public and private sector organisations' intended use of the scheme.

This is an update on the interim estimate published in October 2005 which stated that, at that time, at least 163 million verification transactions could be anticipated at full rollout but that figure could be exceeded considerably. The increase in the current estimates arises out of further work conducted with stakeholders, which provided greater certainty to allow a higher estimate to be assumed. The Identity and Passport Service's User Integration and Marketing teams are continuing to engage with stakeholders to deliver further updates of volume estimates.

While the definitive estimate of transaction points is still evolving and depends on several factors, the programme currently estimates that approximately 44,000 user organisations will seek accreditation to use identity services, including finance sector organisations, employers, and government agencies.

It is important to note that one Government department or commercial organisation may constitute multiple user organisations as it is envisaged that accreditation should be provided on a unit-by-unit basis, rather than to a Government department or parent company as a whole. This reflects the different functions, operation processes and technological standards operating within Government department or commercial organisations.

However, rather than developing the Scheme's assumptions around a fixed number of transaction points which is potentially difficult to predict precisely, it is more important to ensure the solution that is implemented in such a manner that it can be scaled to the demand required. This is being reflected in requirement setting in advance of procurement to ensure that this is reflected in the final design of any bidder.

8. To reiterate the points made at the public hearing, the Identity and Passport Service is not performing trials of the *specific* technical solution that will be implemented for National Identity Scheme as this solution will be decided as part of the procurement process and selection of suppliers. As described in Q9, testing will take place as part of the procurement process.

As mentioned, the Identity and Passport Service, in the context of the introduction of facial recognition biometrics, has conducted testing of the performance of facial recognition systems (current FRS2 trial), which tests the capability to recognise faces with varied poses, disguises and aging. A test population of approximately 300 is being recruited and tested against a database of 23,000 images. The results are currently being analysed. We have also conducted testing of the capability of facial and iris systems to resist spoofing attempts, which was carried out at the National Physical Laboratory. These results are confidential for security reasons. Finally, we have also conducted 'benchmarking' of the IND IAFS fingerprint system to establish a base-line performance for procurement of an improved system. This data is currently being analysed.

In addition, biometric technology is well tested. For example, the National Physical Laboratory in the UK and the National Institute of Standards & Technology in the United States perform very well-respected testing programmes for biometrics.

Furthermore, large scale biometric programmes are already in existence and we are also learning from the operational use of biometrics in other schemes both here and abroad.

9. We intend to undertake extensive testing of the biometric solution both during procurement and the build phase of the programme.

We are taking advice from the Biometrics Experts Group on the content and timetable of our biometric testing programme. These proposals have been presented to the Biometrics Assurance Group, chaired by Sir David King.

These tests planned are:

1. A live enrolment intended to simulate an actual ID Card enrolment. The test will be a competitive trial of bidders' proposed solutions and will enrol and verify approximately 3,000 people, including a large special-needs group. It will test the quality of recorded images, verification performance, usability and spoof resistance. In contrast with the UKPS Biometric Enrolment trial which was a wide-ranging trial examining areas of process timing and customer perception, this is designed to be highly targeted technical trial. 3000 people is the minimum number needed in order to achieve statistically significant results when examining verification performance.
2. A large scale matching test using pre-recorded biometrics intended to provide statistical information on the relative performance of bidders' matching algorithms.
3. A large-scale live enrolment to confirm statistically that the solution will be capable of performing correctly when the National Identity Register is fully populated.

10. In addition to the work mentioned in the answer to question 3 and ongoing monitoring of research, testing and development of biometrics internationally, the Identity and Passport Service is currently contributing funding to the EU Minutiae Interoperability Test research programme. The project aims to deliver strategic research targeted at testing and improving the interoperability of minutiae-based fingerprint systems in time to meet the needs of EU policy legislation.

The trials documented in the answer to question 9 will provide vital new information on fingerprint performance,—large scale performance, verification performance, enrolment and image quality, spoof resistance, usability and inclusivity.

11. Advice contained in the British Computer Society's report "*The Challenges of Complex IT Projects*" are integrated into the Identity Cards Programme in a number of ways.
Managers within the Identity Card Programme review major reports or research relevant to their functional specialism as a matter of course and share important findings with functional teams in team meetings or one-on-ones where relevant. If necessary, the results of such reviews are escalated to the wider programme through its governance structure. In addition, key reports connected with project management and delivery, such as this report, are scrutinised by the Office of Government Commerce. Indeed, OGC contributed to the development of the BCS report. Key learning points are then reflected both in OGC's own publications

and in the Gateway Review Process. As the Identity Cards Programme is subject to the Gateway Review Process, the lessons learnt from such reports have been integrated and form part of the criteria against which it is judged in such reviews.With respect to this specific report, the recommendations from this report are similar to those from the OGC's"Common Causes of Project Failure". The lessons from this are routinely used in the governance of the programme and new projects are reviewed against these common causes of failure at their inception, for example.

"*The Challenge of Complex IT Projects*" report can be found at:
http://www.bcs.org/upload/pdf/complexity.pdf.

12. While we have robust assumptions on the volumes of enrolment data, based on the number of people likely to be enrolling for an ID Card every day and the operating hours of the enrolment centres, the verification volumes, in particular the peak verification load and the distribution of load over time is harder to assess with a high degree of confidence. We are exploring with Qinetiq, based on their considerable experience in this area, what help they can give us in validating our assumptions and suggesting model technical architectures which are tolerant of high data volumes and variations in data volumes. There are not yet finalised scope and timescales for this project.

13. The bulk of the Identity Card Programme's advice on technical and biometric areas is from technical experts within the programme (civil servants and consultants) and related government programmes (including IND (ARC, Biometric Residents' Permits), PITO (IDENT1), the IPS passport projects (e-Passport, Facial Recognition Pilot)), and from the biometrics experts who make up the Biometrics Experts Group (see earlier written evidence for the membership of this group), and from government experts (principally from CESG) in the fields of cryptography and secure computing. Our contact with industry has been to share the high-level intentions of the Identity Cards Programme with companies and invite their reaction and feedback, and also to question them on specific technical areas. A list of participating companies in these seminars is listed below:

VERIFICATION SYSTEMS SEMINAR:

3M Health Care Limited
ARM Limited
Bayer Polymers
Computacenter (UK) Ltd
ECA
EMEA Architects Office
FFW
Giesecke & Devrient GB Ltd
LogicaCMG Plc
Marconi Selenia Communications Ltd
National Identity Cards
Novell UK
OGCbuying.solutions
Ovum Limited
Sagem Communications UK Ltd
Tata Consultancy Services
Triad Group Plc
URU Technologies UK Ltd
Advantage Business Group
Atkins Management Consultants
BT Group Plc
CSC
EDS
Entrust (Europe) Limited
Fujitsu Services Ltd
IBM United Kingdom Limited
Mantix Limited
Methods Consulting Ltd
Nortel Networks Ltd
Oberthur Card Systems Ltd
Oracle Corporation UK Ltd
PCCW (Europe)
Senselect Ltd
TIBCO
Unisys Limited

SECURITY SYSTEMS SEMINAR

3M Health Care Limited
Advantage Business Group
Atkins Management Consultants
BT Group Plc
Cornwell Management Consultants Plc
Daon
Detica Ltd
Eads Defence Security Systems Ltd
EDS
Entrust (Europe) Limited
Fujitsu Services Ltd
Hewlett Packard Ltd
LaserCard Systems
LogicaCMG Plc
Marconi Selenia Communications Ltd
National Identity Cards
Northrop Grumman Information Technology Limited
Oberthur Card Systems Ltd
Ovum Limited
Accenture (UK) Ltd
ARM Limited
Bayer Polymers
Charteris Plc
CSC
Desborough Associates
Digimarc ID Systems
Ecebs Limited
EMEA Architects Office
Experian Ltd
Giesecke & Devrient GB Ltd
IBM United Kingdom Limited
LINK Interchange Network Ltd
MAOSCO Ltd
Methods Consulting Ltd
Nortel Networks
Oracle Corporation UK Ltd
PCCW (Europe)
Senselect Ltd

Sapior Ltd
Serco Justice
Steria Limited
Syntegra Ltd
Triad Group Plc
URU Technologies UK Ltd
Voca Limited
SiVenture
Sun Microsystems Ltd
TIBCO
Unisys Limited
Vega Group Plc
Xansa Plc

The first of these types of contact has been through a number of events hosted by Intellect, each one focussed on a specific area of requirements. The second has involved specific questions sent to selected companies to provide detailed information on market capability. For example, we have met with 15 companies involved with biometrics and have undertaken market sounding activity in relation to biometric matching performance and card durability. This contact has taken place in accordance with OGC (Office of Government Commerce) procurement rules.

The bulk of advice on a day-to-day basis is provided by the members of the programme team and the external advisors working as part of the team. At appropriate times external advisors are asked to assure the work of the programme and to provide input on specific areas.

Reports generated from workshops, surveys, studies, etc. by the programme team and evidence used to inform costing assumptions in our business case and to influence functional and non-functional requirements and interoperability requirements and advice provided to ministers.

14. I have noted your request for copies if the OGC Gateway Reviews to be provided in confidence to the Committee. As you may know, OGC Gateway Reviews are provided in confidence to the Senior Responsible Owner. They are candid assessments as to what action is needed in order for a programme or project to proceed to the next stage. I share OGC's concern that provision of these reports to a wider audience—whether in confidence or not—will put the Gateway process at risk and lead to review teams and people interviewed during the review "pulling their punches".

I am therefore unable to comply with your request, however I have set out the timeline for the Gateway reviews which have taken place. If the issues set out by the review team in the preceding report had not been resolved to its satisfaction, the subsequent review would not have taken place. I hope therefore this reassures the Committee that the Gateway process is being adhered to by the Identity Cards Programme.

Gateway Zero (Strategic Assessment) completed on the 30 January 2004

Gateway One (Business Justification) completed on the 18 July 2005

Gateway Zero (Strategic Assessment) completed on the 14 January 2006

Gateway Two (Procurement Strategy) completed on the 11 April 2006

I should remind members of the Committee that multiple Gateway Zero reviews take place throughout the life of a project or programme as it develops.

In addition, you requested a copy of the Programme's risk register from the last 12 months in confidence. The register is a dynamic tool which is constantly reviewed and updated to reflect changes in the programme. Most of the risks in the register do not relate to technical issues which are of most relevance to your enquiry, rather they focus on areas such as implementing business change, financial and commercial risks. As such, I regretfully decline your request to provide the risk register to the Committee.

However, I can assure the Committee of our approach to risk by pointing to the Gateway reviewers satisfaction with our approach to risk. If they were not satisfied with this approach, further reviews could not have taken place.

15. *Overview of the different stages in the programme*

There will be several separate procurements for different parts of the scheme, each with their own timetable. This overview is based on the process for the NIR (National Identity Register) and associated technology package, which is the largest and most complex of the procurements. Other procurements may follow a slightly different process according to individual requirements.

Stage	*Purpose*	*Key activities in this stage*
Strategy & Scoping (Pre-OJEU)	To ensure the rationale for the procurement, its approach, strategy and scope of the services required are all clearly defined and properly authorised.	— Develop the Business Case — Develop the Procurement, Commercial and Evaluation Strategies — Market Sounding activity to test the viability of the Procurement Strategy — Preparation of the pre-qualification questionnaire (PQQ) and supporting documents — Set up Programme Governance — Prepare for OGC Gateway Reviews

Stage	*Purpose*	*Key activities in this stage*
Commence Procurement and Pre-Qualification	To select only those potential suppliers who meet the IPS security requirements, who can demonstrate track record of successful delivery of the required services and whose financial and commercial risk profile is appropriate for the IPS to consider contracting with them.	— Publish Prospectus — Issue OJEU Notice — Bidder Conference — Issue PQQ — Evaluate responses and short-list — Debrief bidders — Ongoing preparation of the PITN documentation
Preliminary Invitation to Negotiate (PITN) and solution refinement	To enable bidders to gain an understanding of the requirements, propose their solutions and begin solution testing.	— Issue PITN — Manage bidder information & queries — Develop cost comparators — Finalise evaluation model and process — Bidder workshops to develop solution — Evaluate bidders responses to PITN — Optional down-select at this stage — Draft FITN documentation
Biometric Technology Demonstrator and Database Tests	The purpose of the testing is to provide assurance on the biometric elements of NIR package. Results from the testing will be fed into the requirements, where appropriate.	— Testing will occur throughout the PITN, and FITN stages. There are also likely to be additional tests for other elements of the solution, to be determined by the Test Strategy.
Final Invitation to Negotiate (FITN)	To ensure bidders have the maximum opportunity to propose solutions that will meet the requirements fully, and agree the overall shape of the contract.	— Issue FITN to bidders — Continue to populate the contract and its schedules — Continue clarification and solution development — Complete the testing phase and provide analysis of the results — Evaluate the FITN response & select the most appropriate 2–3 bidders to invite to detailed negotiations — Prepare for the negotiations stage — Issue of final requirement
Negotiation	To negotiate with successful FITN respondents to agree service requirements and contract terms against which they will be asked to submit their Best and Final Offer (BAFO)	— Due Diligence by bidders on the relevant data — Negotiation with short-listed bidders to resolve risks and issues identified during FITN evaluation — Issue BAFO — Evaluate BAFO response and select Preferred Bidder — Prepare for Contract Award
Contract Close and Award	To finalise the contract ready for signature, to finalise build and test plans and to make an authorised the decision to award the contract to the new supplier	— Close contract issues and financials — OGC Gateway 3 — Approve decision to award — Finalise plans for the build and test stage — Final Business Case to confirm the agreed contract & price provide VFM — Sign contract
Build and Test	The objective is to move successfully to the point where the new service can be provided by the supplier	— Service provider develops systems — Progressive testing and trialling — Readiness for service checks
Operation	To commence operation of the new service under the contract, and manage and maintain the service to deliver the required performance and benefits over the duration of the contract	— Implement new client arrangements — Start new service — Manage delivery of benefits — OGC Gateway 5

This will be followed by continuous monitoring and improvement, change control, ongoing security accreditation, technical refresh and re-specification.

16. You asked for a breakdown of technology costs in confidence. This has been provided.

Detailed assumptions on technology and the costs of the technology are created that support reference models and the scheme requirements. These are based on and validated by a number of sources and expert advisors, and as a whole, form the cost model and business case. For example, in the case of the timing for the biometric enrolment process, our assumptions on this were informed by timing data coming out of the UKPS biometric enrolment trial and other sources. These data in turn became evidence for the costs model and will allow us to set appropriate, challenging requirements to the market.

17. To support programme decisions and aid in scheme design we have carried out nine separate pieces of social science research in the years 2004 and 2005:

— Omnibus research was carried out in February, April, October and December 2004.

— Two pieces of qualitative research were delivered in December 2004 looking at "Special Needs Issues" and "Citizens" Views on Proposed Customer Propositions'

— Two pieces of quantitative conjoint research were published in October and December 2005. The first assessed UK citizens' and user organisations' views on the scheme. The second assessed Foreign Nationals' views on the scheme.

In addition the UKPS Biometric Enrolment Trial gave valuable evidence on customer perceptions and attitudes, and we have conducted substantial reviews of demographic and geographic information for the purposes of improving our models of identity card roll-out and usage.

Advice on social science studies (qualitative and quantitative research) has been gained through a number of different sources dependent on its nature:

— Statistical advice and a review of all published social science work has been received from the Research Development and Statistics (RDS) units within the central Home Office and the Immigration and Nationality Directorate (IND) for issues relating to Foreign Nationals.

— Advice on research requirements: The Identity and Passport Service (IPS) Marketing and Communications team has significant experience in working with social science studies, and as such has provided advice to the scheme on when issues should be informed by research and how best to use research.

— Advice on commissioning of research and ensuring maximum value is gained from social science has been delivered by the Central Office of Information (COI), the Government's centre of Excellence for Marketing Communications. The third party research agencies which have undertaken the fieldwork have been sourced through COI's framework agreement and as such the agencies have been vetted for their "best practice" approach. For example, the two core pieces of social science research carried out in 2005, "British Citizen Trade-off Research" and "Foreign Nationals Trade-off Research" (both published on the IPS website) were conducted by Taylor Nelson Sofres (TNS) on the Home Office's behalf. TNS is one of the world's leading market information groups with over 14,000 full-time employees across the world and they provided continuous advice throughout the running, analysis and write-up of these two important pieces of social science research.

Social science studies have been used extensively to guide the decision making process within the programme:

— Research has been used to guide scheme design on issues such as price acceptability and acceptable customer time commitment.

— It has also been used to support business case assumptions on volumetrics and likely customer behaviour.

— From a marketing perspective social science has also been used to guide the external marketing strategy by ensuring it is developed to address the public's issues and concerns.

The mechanism for incorporating the result of social science work into the programme is predominantly a robust change control process. Assumptions are validated through research and when the research rejects a current assumption a change request is raised. All our marketers on the programme are also thoroughly briefed on the research findings and provide direct support into different work-streams. As such, they will share the findings across the programme.

18. The Independent Assurance (IA) Panel provides oversight of the programme's ability to deliver the scheme. Whereas other assurance mechanisms such as Gateway reviews measure the strengths and weaknesses of the programme at a specific point in time the IA panel is complementary to this and is more closely involved with the programme and provides ongoing assurance.

The Panel consists of individuals with a vast range of experience of large scale projects and organisations from across the public and private sector. The membership of the panel is:

- Alan Hughes (chair) Former CEO of First Direct Bank
- Malcolm Mitchell Director of Interleader Limited
- John Clarke Former Director of Group Technology for Tesco
- Fergie Williams Former CIO of HSBC's European Businesses

The panel has covered a wide range of topics, including Security, Fraud, Data Integrity, Systems Process Architecture, Marketing, Organisational change, and Risk. The chair of the IA panel sits on the monthly Programme Board, providing the Board with the conclusions of reviews conducted by Panel members on key decisions and papers before the Board.

No significant paper is passed by the Programme Board without first having been reviewed by the IA Panel. Significant papers the IA Panel has reviewed in detail recently include:

- Communications Strategy
- Commercial Strategy
- Procurement Strategy
- Outline Business Case
- Marketing Strategy

Furthermore, the chair of the Independent Assurance Panel is involved as a contributor to the OGC Gateway Process reviews, allowing the Panel to also express their views to other independent reviewers.

19. Use of a "modular IT architecture design approach" will reduce risk to the programme by allowing components to be designed and built separately, having first been defined in terms of their inputs and outputs and their performance characteristics. This also allows the technology to evolve as the needs of the scheme change. If a modular approach is adopted, functional modules can be more easily replaced than if their functionality was embedded in a single, monolithic, system.

This follows standard best practice in a programme such as the Identity Cards Programme. This is reflected in the recommendations of the specific recommendations on modular architectural design raised in the BCS's "The Challenge of Complex IT Projects" on page 29. As noted previously, such advice is also reflected in OGC recommendations more generally.

20. While there are assumptions of technical refresh periods which underlie the components of the National Identity Scheme, the actual renewal and refresh times will depend on the precise technology procured from suppliers.

As noted under 16, detailed assumptions on technology and the costs of the technology are created that support reference models and the scheme requirements. These are based on and validated by a number of sources and expert advisors, and as a whole, form the cost model and business case.

21. The Identity and Passport Service programme and project risk management policy draws on experience and best practice from across the public and private sector including the Office of Government Commerce (OGC) Management of Risk (MoR), HM Treasury Orange Book, the Institute of Risk Management and the Government Communications Head Quarters (GCHQ) as well as from its own experience of project implementation. The policy has been developed by the IPS Programme Control Office Risk Management team, who have significant private and public sector experience; several of the team also have professional risk management qualifications. This team is "embedded" within the constituent projects, enabling a consistent and professional approach to be communicated and implemented.

Furthermore, advice on the Programme's approach to risk management is obtained throughout the development of the Scheme through the OGC Gateway process, which provides practical experience and lessons learnt from the public sector, as well as through the work of the Independent Assurance Panel, which provides experience and advice from private sector background as well.

More specifically, specialist advice is used to mitigate and track risk in specific functional areas within the Programme. For example, key decision papers as well as security risks and issues are raised to and reviewed by the programme's Security, Fraud and Resilience Board which includes representatives from CESG, fraud experts, the programme's security accreditor from CSIA and law enforcement agencies. Such reviews are fed back to experts working with the Programme with recommendations for incorporation into the Scheme's future development.

22. The mechanisms to be used by Identity and Passport Service will not be substantially different from those used prior to the formation of IPS documented in the responses to answers 13 and 17 and in sections 3.6 to 3.14 of the memorandum of evidence submitted by Sir David King to the committee earlier this year. As the CEO of Identity and Passport Service will also have a role within the Home Office as Director General Identity Services and will sit on the Home Office's Group Executive Board, the procedures and facilities in place for the Home Office will remain available to the Identity and Passport Service.

23. Our involvement with international Identity Card schemes has been ongoing through the lifetime of the programme, starting with visits to EU partners before the consultation paper went out. We have continued to share experiences with EU partners and with the US. We also engage with other schemes and projects related to identity cards though international conferences, standards organisations, and bodies such as ICAO (International Civil Aviation Organisation).

The visits to the identity card schemes in Hong Kong and the Philippines. These visits covered:

- Enrolment processes
- Biometric performance
- Layout of enrolment offices
- Enrolment timings
- Checks made on applicants at enrolment
- Location of enrolment offices
- Verification checks
- Card production and card costs
- Use of PKI
- Procurement principles

Information gained from these visits has been used within the programme to validate our business case assumptions and to inform our requirements.

24. We have met with officials from the US Department of Homeland Security (DHS) on a number of occasions. We visited officials in January 2004 and briefed them on our plans for biometric ID Cards. There was further contact and ongoing dialogue through 2004 and 20005 both directly and through the Biometrics Working Group.. An official from the DHS presented a summary of the department's work to officials from the Identity Cards Programme on 24 February 2006 and officials from the Identity Cards Programme visited DHS for demonstrations and meetings on the 10, 11 and 12 April. As this visit was recent, the conclusions have not yet been properly written up but this visit did serve to demonstrate the feasibility of running a highly reliable biometric enrolment and verification system with 40-50m individuals enrolled.

In the oral evidence session on 22 March the chairman of the committee stated (Q272 in the transcript), that in terms of biometrics for ID cards, the Department for Homeland Security had said that "the technology was not there". During this visit we put this to several very senior officials responsible for the operation, development and management of US-VISIT, They rebutted this assertion strongly and pointed to the marked success of the technology employed in US-VISIT which allows rapid 1-to-many matching of fingerprints on a database of 40–50m with negligible impact on process times, and which processes 125,000 verification transactions per day at present.

25. A public communications strategy was developed for Identity Cards Programme in co-operation with the UK Passport Service. Following the creation of the Identity and Passport Service, this now forms part of the wider communications activities of the organisation. This strategy also reflects emerging technical changes that will be common to both the development of the passport and the introduction of the identity card.

The Identity and Passport Service recognises that, as biometric technology is increasingly used to improve identity authentication and document security, we need to ensure that our customers understand what biometrics are and how they will be used. This is an important element of our ongoing marketing and communications strategy. Examples of our marketing and communications activity to date include the following:

- A series of regional biometric roadshows took place in September/October 2005 to raise awareness amongst the general public about biometrics and changes to passports. Members of the general public had the opportunity to have their iris and fingerprints recorded and verified.
- To prepare for the introduction of e-passports this year, a customer leaflet has been produced to explain what biometrics are, how facial biometrics work, and what information will be held on the chip. This is also available on our website www.passport.gov.uk . A copy of this leaflet is provided in Annex J (not printed).
- A separate leaflet has also been produced which we send to customers with their new e-passport. This explains why the IPS is introducing this new style of biometric passport to help fight fraud and forgery. A copy of this leaflet has been provided in Annex K (not printed).
- The IPS website is an important channel for providing information to our customers and other stakeholders about biometric technology. The site includes questions and answer sections about biometric passports and biometrics generally.
- A DVD has been created that helps explains the planned implementation of the Identity Card Scheme, which has been used in consultations with the public, such as the Programme's consultation with faith communities. An abridged version of this DVD has been placed for

download on the IPS identity cards website (www.identitycards.gov.uk). Copies of the full DVD was placed in the House of Commons and House of Lords libraries during the passage of the Identity Cards Bill through Parliament. A further copy has been provided to the Committee.

— The media is an important channel for raising awareness about biometric technology. IPS has issued various press releases over the last 12 months which have explained the need to improve the security of travel documents through technological advances which are being adopted across the world.

As the IPS continues the delivery of the key changes already underway to improve the passport document and issuing process, and develops the National Identity Scheme, our marketing and communications strategy will continue to incorporate key messages and activities to build awareness and understanding for our customers and other audiences.

May 2006

APPENDIX 16

Memorandum from Professor Anne H Anderson, University of Glasgow

"Scientific Advice, Risk and Evidence: How the Government Handles Them"

1. I welcome the opportunity to provide evidence to the committee as it deliberates this topic and the case study of the technologies supporting identity cards. I note that to date the committee has received little evidence regarding social science. I also note that the Home Office has indicated that they have made extensive use of "social science studies have been used extensively to guide the decision making process within the programme:

— Research has been used to guide scheme design on issues such as price acceptability and acceptable customer time commitment.

— It has also been used to support business case assumptions on volumetrics and likely customer behaviour.

— From a marketing perspective social science has also been used to guide the external marketing strategy by ensuring it is developed to address the public's issues and concerns.

The mechanism for incorporating the result of social science work into the programme is predominantly a robust change control process. Assumptions are validate through research and when the research rejects a current assumption a change request is raised. All our marketers on the programme are also thoroughly briefed on the research findings and provide direct support into different work-streams. As such, they will share the findings across the programme".

2. Although this input from social science may well have been valuable to the Home Office with reference to the development of the National Identity Scheme, it is a narrow perspective on social science and where the social sciences could be used to improve the scheme.

3. I direct a major research programme (PACCIT) with leading academic researchers from the social and computing sciences in universities across the UK. When the research councils and the DTI committed to fund the PACCIT initiative they did so in the recognition that IT systems often fail to deliver their intended benefits because the systems have been designed with a lack of understanding about the users' needs and the context of use. Good multidisciplinary research drawing on both social and computing science is needed to help overcome these problems. From my knowledge of the development of the National Identity Scheme, there is a real danger of both of these problems. The challenges of implementing the various biometric technologies have been the focus of concern, and it appears that less attention has been given to the challenges of how to design and implement the system in ways that are usable, useful and appropriate.

4. If the further development of the scheme is to be successful, it will be important that the Home Office draws on expertise from a suitable range of expertise from social and computing science to ensure the National Identity Scheme is designed and implemented to meet these criteria. The specification for the system and the trials of the proposed technologies referred to in oral evidence to the Committee on 22 March 2006 must be broadly scoped to include not only the technologies in isolation, but the system as a whole. Sufficient time must be included to refine the design in the light of evidence from realistic trials of the system in operation. It will be important to ensure that the relevant expertise is available to gather and analyse this data on the whole system performance. The Home Office may need to engage independent experts to help evaluate the trials and help feed the information back in to the process of refining the design.

5. One important aspect of this process is the enrolment process. The performance of the various biometric technologies *per se* is important, but it is the performance of these technologies in the varied intended enrolment settings, with the staff who are likely to be operating the systems, with the range of likely potential customers, that is key. The Home Office state they have taken some advice from social scientists

about the "acceptable customer time commitment". In addition the trials will need to consider and monitor the complete customer and staff experience of enrolment, to ensure the system works in an efficient and acceptable way, or to determine what alterations are needed to make it do so.

6. The need for such considerations can be illustrated with reference to the information and case studies provided on the Home Office (www.identitycards.gov.uk). The site includes information about how ID card will work in practice and lists a wide variety of organisations that are expected to use the scheme to check the identities of their customers. These range from banks, Royal mail, Universities, airlines, vehicle and property rental companies, retailers of all kinds including internet based companies, libraries and video/DVD rental companies. A moment's reflection on these very different contexts of use, highlights the design challenges this very varied set of requirements presents. The Home Office web site acknowledges in its illustrative everyday examples, that these kinds of organisations will need different levels of security but the different contexts require more consideration than this.

7. One of the complications in designing and implementing an effective National Identity Scheme, is first identifying who are the prime "users" of the technology, whose needs the scheme should be designed to serve. Some of the benefits described by the Home Office are described in terms of benefits to the customer, in terms of the speed and efficiency with which they can establish their rights to certain services. In the examples however the focus seems more on the needs of the service provider to check identification. This may reflect the nature of core Home Office responsibilities for services such as crime and immigration, where the "customers" and their needs are not particularly salient. The important point is that the design specification that may emerge from this standpoint, may not lead to appropriate or acceptable solutions in other areas.

8. One of the case studies illustrates this, and the point made by Professor Thomas in his oral evidence to the committee on the need to distinguish between authentication and identification. (3/5/06 response to Q489). To use the ID card to prove you are old enough to buy alcohol or obtain an-over 65 discount, you need to establish that you have reached the legal age. You do not as the case study describes, need to have the shop assistant confirming the customer's identity or date of birth. Many people would regard the latter as an invasion of privacy. The key point I want to make is that the Home Office needs to be more sensitised to these social concerns and ensure that the system is designed to ensure what the European Courts are defining as "a reasonable expectation of privacy". This sensitivity needs to extent to scoping the system specification appropriately. The card should not make available to service providers more information than they genuinely need. So for example the card might indicate, without the need to access the data base, that someone is over 18 but not their date of birth.

9. The list of potential user of the scheme include "retailers of all kinds" which again has some worrying implications for privacy as well as raising similar design challenges. In many cases all retailers require to know is that the customer has the means to pay for the goods or services. The identity of the customer might be very valuable information for retailers for marketing or customer profiling but the system should not allow access to more information than is needed. The Home Office web site provides assurances that identity checks can only be conducted with the customer's consent, and that these checks will simply confirm "your identity or other known facts, such as your address details from NIR". The scope of the "other known facts", and to whom they are made available, needs careful consideration. The design of the system has to ensure that even when consent has been given, the system allows access to the minimum necessary information. The very wide variety of potential contexts of use, make this design requirement essential.

10. *Multiple Identities.* In social science it is acknowledged that we all have multiple roles and identities. We are parents, employees, spouses, citizens, sufferers from various illnesses, football fans, opera lovers, recovering alcoholics etc etc. We quite legitimately might wish to keep these roles and identities separate. Both English and Scots Law allow individuals to be known by a variety of names. For some individuals this is not just a matter of personal preference but a very serious matter. To take just three examples, for women leaving abusive relationships or for individuals being stalked, or for celebrities, apparently innocuous identity information about name(s) and addresses may be very sensitive. If such information has to be revealed and verified in a wide range of service encounters from libraries to video rentals to travel agents, serious invasions of privacy may occur. The design and implementation of the National Identity System must be flexible enough to protect information individuals consider sensitive or to allow other forms of verification of entitlement to services.

11. In summary

The National Identity Scheme is a very challenging project. It is a complex socio-technical system and to be effective will require that the Home Office considers the social as well as the technical dimensions. The effective design and implementation of IT systems requires among other things, an understanding of the users' needs and the context of use, and this information needs to feed into the design of the system. At present the Home Office may not be very well connected to sources of independent expertise on the social and computing sciences, which could be useful in helping them scope the requirements of the proposed system. The design of the system should ensure that the system respects the privacy of individuals, and enshrines the "reasonable expectation of privacy". The design should support the distinction between authentication and identification and should allow service providers to access only necessary information.

It will be essential to conduct substantial and realistic trials of the system. These should be independently evaluated, including in terms of the customer and staff experience. The data should feed into refinements to the proposed system.

12. The views expressed are my own. Some of the concepts in this evidence emerged from discussions with colleagues on the DTI Foresight Project on Cyber Trust & Crime Prevention, (see R Mansell & B Collins (Eds) *Trust and Crime in Information Societies* (2005). Edward Elgar: Cheltenham) and the Royal Academy of Engineering Working Group on *Dilemmas of Privacy & Surveillance* (report to be published this year).

June 2006

APPENDIX 17

Supplementary evidence from the Government

QUESTION 1

During the evidence session on 7 June 2006, Paul Wiles stated that he does not have responsibility for ICT in the Department (Q1131). Through informal inquiries to the Home Office we have been told that the Chief Information Officer, Vincent Geake, has responsibility for ICT advice. We would be grateful if you could confirm this information and outline the CIO's involvement in the ID cards programme, for example the meetings attended, forms of advice given

The Home Office CIO, Vincent Geake is responsible for providing advice about ICT strategy, but not about ICT delivery within programmes.

We engage with Vincent Geake principally through his attendance of meetings of our Programme Board (he has attended meetings in March, April and May) and also through HOSIS (Home Office Strategic Identification Systems) and its subgroups.

Vincent Geake and the CIO's Office are working through HOSIS on a component model of all Home Office identity systems to identify areas of overlap and areas where sharing of infrastructure and resources are possible.

The ID Cards Programme is also represented at the CTO (Chief Technology Officer) Council and the CIO (Chief Information Officer) Council along with CTO and CIO representatives from across government. Key areas for these councils in the near term are a roadmap for how the shared services agenda (outlined in last year's "Transformational Government" paper from Cabinet Office) will be delivered, and the creation of a secure Enterprise Architecture framework for government IT (ie a common architectural model for Government IT systems).

QUESTION 2

Please explain the relationship between the Chief Information Officer, Vincent Geake and the Departmental Chief Scientific Adviser, Paul Wiles. How often do they meet? Have they discussed the science and technology involved in the identity cards programme?

Vincent and Paul meet every two weeks. Their discussions focus on the strategic role of the Identity Cards programme and its relationship with other Home Office initiatives.

QUESTION 3

In response to our letter of 29 March 2006 the Home Office answered Question 17 by saying that "the Identity and Passport Service (IPS) Marketing and Communications team has significant experience in working with social science studies, and as such has provided advice to the scheme on when issues should be informed by research and how best to use research". Please provide details of the scientific expertise in the Marketing and Communications team and the advice that it has provided to the scheme regarding social science research.

Three Marketing and Research specialists within the IPS Business Development Directorate are responsible for providing guidance and management of social science input. All have social science degrees with course elements collectively covering quantitative and qualitative research methods, statistics, computing, econometrics and modelling. They have wide experience of applying this knowledge as marketers and researchers, gaining insight into customer needs and motivations and using this to refine product and service design in both the public and private sector. They have particular experience of Trade-Off research and modelling. Public sector examples include.

— Customer insight (both qualitative and quantitative research) and demand modelling for National Savings and Investments to help with the development of a Business Case and product definition for their ISA savings product. Subsequent sales met the two year forecast.

— Qualitative research for National Savings and Investments into customer perceptions and needs in relation to Premium Bonds, leading to a new marketing strategy for Premium Bonds. Sales of Premium Bond radically increased following implementation of the strategy.

The team has also been supported by Research Development and Statistics from the Home Office Communities group, and Immigration Research and Statistics Services, part of IND.

The expertise that has been provided to the scheme regarding social science research has included:

— recommendations regarding the types of research best suited to answering Identity Scheme questions (eg the use of trade off research to help guide scheme design and volumetric modelling);
— the specification and implementation of the research studies;
— advice on sample sizes and quotas to ensure statistical significance on results;
— advice on discussion guide design and on questionnaire development;
— interpretation of findings and modelling of data; and
— drafting of research reports for publication.

This advice has been supported by leading global research agencies delivering scheme research (eg Taylor Nelson Sofres on quantitative trade off research for British Citizens and Foreign Nationals and Cragg Ross Dawson for qualitative research on scheme opinion). The Central Office of Information have also been responsible for the management of all social science research studies undertaken by the scheme, and have provided quality assurance and contract management support to the specialist team.

QUESTION 4

In evidence to the Committee on 14 June, the Minister stated that all risks must be mitigated. Please provide details of the risk mitigation strategy within the identity cards programme and explain how different risks such as time, money and functionality are prioritised

The programme's risk process is based on the OGC's approach whereby all risks have named owners. These are identified as early as possible after the risk is articulated and are selected because of their ability to drive forward the activity needed to address the risk. The owner, where appropriate, assesses the risk for the impact on budget and schedule. The Risk & Issues Team in the Programme Control Office provide recommended guidelines for this assessment based on bandings. For example, an impact of 3% on a budget would be considered Negligible whereas an impact of 15% would be considered Catastrophic. The probability of the risk occurring is also assessed either based on quantitative information or the Risk Owner's experience. As far as possible the assessments avoid "feel" and rely on quantitative information.

The information is entered into the Programme Risk tool which calculates an overall score on which to prioritise the risk. This assists the Risk Owner in their decision on the approach to be taken to the risk (eg transfer, tolerate, terminate or treat) based on which the Risk Owner must either design and put into effect a mitigation plan or make a positive decision to tolerate the risk. In all events, until a risk is closed by the Board, it remains the Risk Owner's responsibility. Each risk is assessed on an individual basis and mitigated where possible.

The mitigation plan should address the main impacts of the risk occurring (so if the risk will primarily impact on schedule, the mitigation should address that area in the first instance). The mitigating actions (and activity on these) are assessed by Risk Managers embedded in projects and programme and this is reported upon in the risk log and, where appropriate to the Board along with the assessments of the risk as circumstances change.

In some cases a full quantitative analysis is carried out which runs a Monte Carlo analysis on the information provided by the Risk Owners to determine which risks will impact most on the Programme/ Project overall enabling the Boards to prioritise those risks and allocate resource accordingly.

QUESTION 5

Please provide details of the processes that are used to develop contingency plans within the identity cards programme

Contingency planning is a necessary adjunct to the assessment and treatment of risks which falls into the ambit of the Risk Owner. Contingency planning is not done for every risk but will be done, in line with accepted practice, chiefly based on the severity of the post-mitigation status and overall risk score for the risk. Working with the Risk Manager and Planner, the process is to build a plan to deal with the risk should it mature either where the decision has been made to tolerate rather than mitigate the risk or where the identified mitigation actions are not complete. The Risk Owner is, by definition, in an appropriate position to ensure that the plan can be resourced and an understanding formed of the cost of putting this contingency plan in place which weighs the cost of contingency against the costs incurred by the risk. Where the plans are considered sufficiently complex, specialist planning assistance is obtained from the Planning team.

QUESTION 6

We have received evidence stating that there "is no openly published work from the UK Government into the risks associated with different types of technical models for national ID cards". Have you undertaken such work and if so, why is it not published?

We are developing output-based requirements which encapsulate what we want the ID Cards scheme to deliver—that is, a convenient and secure means for individuals to establish and verify their identities. We are developing technical models of how different parts of the scheme might work in order to test the feasibility of delivering our requirements and to provide a benchmark against which to evaluate proposals from suppliers, but have no plans to publish them.

To publish these models or the risks associated with them would suggest to the market that we had a specific technical solution in mind. This would risk influencing suppliers to base their proposals on these, thinking that this would lead to their proposals being favoured. If this happened we would be losing the advantages of setting output-based requirements—that is, promoting innovation in the supplier community and allowing suppliers the ability to use their specialist technical expertise unhindered by being steered down a narrow technical path.

QUESTION 7

During the oral evidence session on 14 June, the Minister mentioned that the interoperability of the technology between different Government departments was being approached in a number of ways. We would be grateful for more detail on this point. Furthermore, please provide details of the interaction between Government departments regarding the science and technology underpinning the identity cards scheme

Last month the Prime Minister announced the creation of the Ministerial Committee on Identity Management chaired by the Leader of the House of Commons. This will co-ordinate the Government's policy and strategy on identity management in the public and private sectors and drive forward the delivery of benefits. This Committee will build on the work of an ad hoc group of Ministers of State which has met three times to identify cross-Government benefits. In support of the new Committee is an Identity Strategy Management Group, with representatives from all Key Departments at Director General level. Again this group reviews work and positions the work in a wider Identity Management context across Whitehall.

Interoperability depends to a very large part on common technical standards. To this end we are, when setting our requirements, using the work done by the e-Government Unit (eGU) in the e-GIF document (Government Interoperability Framework) which sets standards in the fields of eg smartcards, data storage and communication to facilitate interoperability between government systems.

We are also mandating appropriate international standards. For example we have said that ID Cards which are valid for travel will be compatible with ICAO (International Civil Aviation Organisation) recommendations for machine-readable travel documents. This has been done in close consultation with colleagues in IND and means that the card will be able to be read at border controls by the same equipment used to read the chip-enabled passports.

QUESTION 8

The Committee would be grateful to receive details of consultations that the identity cards programme have undertaken with Local Government regarding smart card technologies and the outcomes of any such consultations

We have engaged with and held meetings with some Local Authority smartcard schemes but our interaction is chiefly through the organisations which have a national perspective on these schemes such as the National SmartCard Project (NSCP) and Government Connect. These organisations have assisted us in finding out more about the appropriate use of smartcard standards and we have discussed common interests such as review of transaction authentication levels.

We have also attended the e-Government Unit (eGU) Smartcard Working Group which includes representation from local and central government and transport schemes.

QUESTION 9

In oral evidence to the Committee on 14 June, the Minister agreed that the majority of benefit fraud is not committed by people that lie about their identity. What evidence does the identity cards programme have that identity cards using biometric technology will tackle benefit fraud?

DWP benefit fraud is committed through a number of means other than the use of false identities This has been consistently stated by the ID Cards Programme (for example in the 2002 Consultation Document, para 4.5, p40).

However our analysis to date with DWP has identified a number of areas of benefit fraud that will be impacted upon by the introduction of an Identity Card:

Identity Related Benefit Fraud/Housing Benefit Identity Fraud

The introduction of the Identity Card is expected to reduce/negate the ability of individuals to have more than one identity and therefore present multiple fraudulent claims to benefit. Improved ID verification supported by biometrics would counter one person holding numerous fraudulent claims to benefit.

However benefit fraud is not necessarily about identity, it is about failing to disclose correct circumstances. The introduction of an Identity Card and information from the National Identity Register (NIR) could help DWP to determine the correct circumstances.

Living Together/Partner fraud and error:

Address data stored on the NIR could help in detecting Living Together fraud and error cases by identifying discrepancies between declared and real addresses.

Housing Benefit Residency / Household Composition Overpayments:

The ID Cards Scheme could make a significant contribution to this area, address data stored could also assist in tackling Non Residency and Household Composition in Housing Benefit (HB).

These benefits are predicated on three key characteristics of the ID Card scheme; Firstly, the biometric verification of individuals which will tie that person to a particular identity; secondly the subsequent address information (tied biometrically to an individual) which will provide a much more robust basis for benefit applications and possible investigations. Thirdly it will rely upon full national roll out of the Scheme and compulsory registration.

QUESTION 10

The Government response to our letter of 29 March 2006 stated that "the mechanism for incorporating the results of social science work into the programme is predominantly a robust change control process. Assumptions are validated through research and when the research rejects a current assumption a change request is raised". In the oral evidence session on 14 June, the Minister agreed to write to the Committee outlining specific examples where changes to policy have been made as a result of the outcomes of social science research.

The following are specific examples of where policy is being guided by social science research:

- "British Citizen Trade-Off Research" published in October 2005 studied the perceptions of travel time to an enrolment centre for members of the public. This was used to guide scheme policy on travel time and enrolment centre locations to ensure travel time for British Citizens is limited to acceptable levels.
- Qualitative research carried out by Cragg Ross Dawson highlighted that if the scheme were to be entirely voluntary (as opposed to one where passports become designated documents under the ID cards scheme leading to a fully compulsory scheme) then public support for the scheme in general would be weakened.
- "British Citizen Trade-Off Research" enabled the team to provide guidance on likely take-up for both a standalone identity card and a combination identity card and passport product. Likely adoption levels were then used to guide business case development and operational design.
- Research has been carried out amongst the public to understand how they would like their identities to be verified in different situations (ie using biometrics, using card and PIN, visual authentication against card etc.) This research is being used in business customer workshops to help guide the development of our requirements.

QUESTION 11

In the oral evidence session on 14 June, the Minister undertook to write to the Committee on the question of whether the identity cards programme would undertake a Gateway Review on the practical and technical feasibility of the project and make such a Review available.

The OGC Gateway review process is designed to examine programmes and projects at critical stages in the lifecycle to provide assurance that they can progress successfully to the next stage. It is not specifically designed to examine in any depth the practical and technical feasibility of a programme. The programme has been through four reviews:

- Gateway Zero (Strategic Assessment) completed on 30 January 2004.

— Gateway One (Business Justification) completed on 18 July 2005.

— Gateway Zero (Strategic Assessment) completed on 14 January 2006.

— Gateway Two (Procurement Strategy) completed on 11 April 2006.

So, for example, the OGC Gateway 1 (18 July 2005) checked that the feasibility study examined:

— A wide enough range of options.

— The advantages and disadvantages for each option to determine its potential for meeting the critical success factors.

— Option appraised in accordance with the principles of HM Treasury Green Book.

— Clear analysis of whole-life costs for each option.

On the question of publishing the content of Gateway reviews, these review reports are provided in confidence to the Senior Responsible Owner. They are candid assessments as to what action is needed in order for a programme or project to proceed to the next stage. There is a risk that provision of these reports to a wider audience will jeopardise the Gateway process and lead to review teams and people interviewed during the review "pulling their punches". Therefore, and in line with practice across government, it is not our policy to publish Gateway reviews.

June 2006

APPENDIX 18

Memorandum from Microsoft

1. Executive Summary

The introduction of identity cards is clearly a decision for HM Government and Parliament to take. Microsoft's only interest is in the practicalities of how fit for purpose the technology will be that will underpin this project. We believe that achieving this goal will be greatly helped by drawing on the expertise available in the IT industry to discuss the technological issues that need to be resolved to ensure successful delivery. The industry has learned many lessons around identity, privacy and security and we are keen to share this knowledge more widely. This is a major project and it is obviously crucial that it obtains the highest security levels possible and works well with existing structures both within the public and private sectors.

We believe the Government policy set out in the *Transformational Government* strategy is a good model: that is to:

> "*create an holistic approach to identity management, based on a suite of identity management solutions that enable the public and private sectors to manage risk and provide cost-effective services trusted by customers and stakeholders." (para 7, page 13, Transformational Government)*

The current phase of the public Home Office consultation process has largely focused on addressing procurement and supplier-related processes and issues. Although this approach is entirely understandable for the initial stages, we suggest that the next stage should adopt the approach taken by the US State Department, which created a model that actively encourages broad, open dialogue in pursuit of improved outcomes.

By adopting a similar approach during the next phase the Home Office will be able to foster a broader, inclusive coalition able to examine the wider issues around alternative architectural models and technologies, comparative risk analyses, and the state of current research combined with measurable objectives and benefits of the scheme. It could also factor in some interesting alternative approaches being developed elsewhere, such as the Austrian Burgerkarte.

Correctly constructed, such consultation need have no implications for any "pollution" (real or perceived) of subsequent procurement processes. Rather, it would help bring into play broader industry expertise to help assist the Home Office with the development of an identity scheme most able to bring sustainable, real benefits to citizens, businesses and the public sector alike.

We have welcomed the approach of open, public discussion taken by the Home Office Minister Andy Burnham, MP. We hope that this is an early indication that the next stage of the consultation process will look to draw on the wider expertise available and commit to take an open approach on what is the best way forward.

2. Sources and Handling of Advice

2.1 The current phase of public consultation by the Home Office has primarily focused on issues of procurement and hence been conducted mainly through trade bodies such as Intellect and EURIM.

2.2 It would be very beneficial to relate the Home Office identity programme to other identity initiatives including across health, local and central government and the private sector (chip and PIN bank cards being a topical example). Such joined-up thinking on identity management could certainly benefit the public sector reform agenda and transformation programme and all of these programmes have specific needs for clarity on identity, from supporting the determination of entitlement to benefits, to clinical audit.

2.3 The industry is clearly willing to share its experiences of developing and managing identity systems. Microsoft has been working with a broad industry coalition to distil a proven, empirical set of principles for successful identity systems. These principles are intended to help bridge the divide between policy aspirations and lower level technical implementation details and hence provide a critical part of the overall infrastructure required. These principles are currently referenced as the "laws of identity" (laws as in scientific principles). We do not claim perfection or any uniqueness of insight in these "laws" but do believe they provide a constructive basis for discussion and debate on ensuring the proper scope of identity systems that will prove sustainable and robust in the long term.

3. Relationship between Scientific Advice and Policy Development

3.1 The original public proposals suggest a centralised technical architecture is being considered, with all validations made online to a single biometric database capable of ensuring unique enrolment (ie the ability to ensure no individuals are enrolled more than once to prevent, for example, a benefits claiming making more than one claim under separate identities).

3.2 As the next phase of consultation is developed by the Home Office, it would be invaluable to develop widespread public discussion on security. In particular, how we can ensure that any system is robust enough to withstand the sort of sophisticated identity theft that is being experienced today let alone what is going to happen tomorrow.

3.3 This public discussion would assist with an evaluation of alternative technical architectures best able to deliver the stated policy requirements and objectives. It would aid the development of UK government studies on the risks, feasibility and comparative merits of centralised versus decentralised identity systems in terms of systems reliability theory, or modern computer security concepts (including the widespread contemporary experience of large scale data breaches, social engineering and phishing attacks).

3.4 In our view, the robustness of the system should lead decisions on everything else. If any given system or solution cannot provide the public with the highest security and reliability levels possible then it should be replaced with one that can. All of the technologies being considered should be put through the same rigorous scientific assessment, preferably with the engagement of experts drawn from across the IT industry.

4. Treatment of Risk

4.1 During the present phase of consultation the risk model has not been made publicly available (it is recognised that some limited parts of the risk model may always need to remain confidential to government to help protect our critical national information infrastructure).

4.2 The overall technical architecture and associated risk modelling is clearly inter-dependent on the policy and business requirements and objectives of the ID Card scheme. Various risk models will need to be evaluated in the light of any technical architectures identified during a next phase of consultation.

4.3 Going forward, we would recommend that there is widespread discussion on the level of risk of different technological options. It is clear for instance that options such as biometrics (whether used for authentication and/or identification) also present sizable challenges. For example, biometrics are not secrets and are increasingly likely to be stored in many different systems, including systems hosted in other countries and under other governance regimes. The likely future ubiquity of biometric information is an important factor in risk assessment. It should be assumed that over time these systems will tend towards entropy. Digitised versions of our biometrics are likely to end up in the public domain as they become more and more ubiquitously used, stored and (potentially) leaked across the world. It should be assumed that they will be readily available to criminals, not just law enforcement and related legitimate agencies. We believe that public discussion and consultation on risk issues such as this would be beneficial in establishing a sustainable, long-term risk model for the proposed ID Card scheme.

5. Transparency, Communication and Public Engagement

5.1 Current formal channels of communication and consultation regarding the procurement process have been largely limited to two bodies: Intellect and EU RIM.

5.2 We understand some selected suppliers have been involved in closer 1-to-i briefings with Home Office officials. It is not known what scientific, technical or other issues have been assessed during these meetings.

5.3 Here again we would encourage wider consultation. It is essential that major industry sectors are consulted on how the ID card will impact on their businesses, especially in identity evaluation. An obvious example here is the banking industry. We believe a broader consultation during the next phase of the Home Office's work could help develop greater clarity and agreement about how and where the proposed ID Cards could be used, for what purposes and—most importantly—the benefits that citizens and businesses would derive from them. A successful scheme will rely upon balancing the needs of public policy, optimised technological design and citizen benefit.

5.4 During a next phase of consultation, inputs from a variety of third parties could be considered and responded to on an evidential and scientific basis. In the USA, public dialogue and debate is openly referenced by the US State Department as being a considerable benefit and having led to substantial improvements in systems design and improvements in both security and privacy elements.

5.5 Closer to home, the Ministry of Defence's Capability Working Groups process is also a useful reference model.

5.6 Microsoft continues to be willing to openly share its learnings and experiences (including as one of the primary attack targets for hackers and criminal gangs) in a non-privileged, non-preferential way to help de-risk and inform the overall ID Cards technology programme.

6. Evaluation and Follow-up

6.1 Information in the public domain which is limited due to reasons of commercial confidentiality makes it difficult to comment on the theoretical evidence base and any adjustments made to it as the programme has developed.

6.2 We believe that the next round of trials should be expanded to broaden the statistics on reliability and modelling operational performance. These trials should further help inform the planning process and hence underpin a successful outcome of the proposed scheme.

6.3 Level 2 identity verification is already achievable today from several agencies such as local authorities, banks and employers as well as the likes of credit reference agencies such as Experian and Equifax, at relatively low cost. Level 2 provides access to over 90% of government services as well as addressing most fraud scenarios relating to identity. The objectives, risks and architecture for ID Cards as part of this broader, holistic identity landscape needs to be more clearly articulated so that it can be formally incorporated into the bigger picture set out elsewhere, such as in the Transformational Government strategy.

In conclusion, we reiterate that the industry is committed to helping share expertise and hands-on experience to help inform the planning and technical architecture of the proposed scheme. We look forward to the next stage of consultation and hope that our comments are taken in the constructive manner they are intended.

January 2006

APPENDIX 19

Letter from Joan Ryan MP, Parliamentary Under-Secretary of State for Nationality, Citizenship and Immigration, Home Office to the Chairman

Responses to Questions from the Science and Technology Select Committee

Thank you for your letter of 11 July. I am glad that you found the briefing you received last Monday useful.

You raised a number of questions relating to the reports of an "early variant" card asking what this was, how it might differ from the existing proposals, what the cost implications might be, and what the argument was that this would be an appropriate first step.

The term "early variant" is misleading in implying that there are firm plans for a different type of card to be issued earlier than others. The plans for ID cards have always been incremental with no "big bang" implementation and the Identity and Passport Service is considering the most appropriate first incremental steps to introduce ID Cards.

There is an ongoing programme of work to ensure a smooth implementation. The Identity and Passport Service (IPS) has already started the introduction of facial image biometric passports and will move next year to interviewing all first time passport applicants. These are essential building blocks in the incremental programme leading to the full implementation of identity cards.

You also asked about the review of Home Office activities. Following the Home Secretary's written statement on 23 May (*Official Report,* column WS 81), a small team was established with the objective of producing a reform plan for the Home Office by the summer recess, in addition to the complimentary work underway on reviewing the Immigration and Nationality Directorate and rebalancing the Criminal Justice System. This review is about reforming the Home Office so that it is able to deliver its core objectives of public protection in an ever-changing world, rather that an analysis of specific policy issues such as the ID cards programme. In this statement, the Home Secretary signalled his intention to report back to Parliament on progress and proposals for change before the summer recess.

The timetabling of the ID cards programme is being reviewed by IPS alongside the plan for reforming the Home Office. The Home Office remains committed to delivering the ID cards programme as soon as possible, starting with biometric residence permits for foreign nationals in 2008.

Finally, on another matter, you asked by email whether it would be acceptable for you to include a reference in your report to the briefing held on the 10 July. Your request asked whether the report could cite the two specific risks covered but without details of the ratings of these risks or of how they are being dealt with. In keeping with my letter of 22 June in which I requested that the briefing be considered confidential, I am content that your report should make a reference to the briefing, but not for the specific risks covered to be referred to. I look forward to seeing your report when it is published.

Joan Ryan

July 2006

Printed in the United Kingdom by The Stationery Office Limited
8/2006 333922 19585