From:
Mr Alan Hughes,
Chair, Independent Assurance Panel, (the Panel),
The National Identity Service (NIS).

To:
Mr James Hall
Chief Executive, The Identity and Passport Service (IPS) and
Senior Responsible Owner (SRO), the NIS

1. Context and Purpose

1.1 In addition to the reviews we have undertaken and the advice we have given at NIS Management Board meetings and other forums, you have asked for this summary of our observations on the programme of work (the Programme) to implement identity cards, the database of biometric and biographical records - the National Identity Register (NIR) and identity verification services[1]; which together will comprise the NIS. Our Panel was created at the recommendation of the Home Affairs Select Committee in 2005, to help assure the Programme.

1.2 The Programme has built a capability to record biometric data and offer identity cards in limited numbers. The first cards were issued on time and budget in 2009. Much of the infrastructure for this launch will be superseded by the high-volume systems you have commissioned. The relatively small-scale launch is a prudent means for you to perfect the design of the full-scale NIS. This eventual infrastructure will also enable 'second-biometric' passports (see 1.5) and replace current passport systems. We support the re-use of existing assets that you propose as part of this. Re-use will help to protect the integrity of the NIS, although it may create issues that may be not have been present if a 'green-field' approach had been adopted.

1.3 It is our opinion that the work done to commission the components of the NIS has been well managed to date although some specifications are incomplete, notably for usage and verification services. You are well aware that the chosen suppliers will now need close management, as will changes or additions to requirements, if the full-scale infrastructure is to be delivered to specification, time and budget.

1.4 We note that the purpose of the NIS has shifted since 2005, as has the national context. The 2006 Identity Cards Act cites national security, crime prevention, immigration controls, prevention of unauthorised working and the efficient provision of public services as benefits, with the power to make card-holding compulsory by designation of events such as renewing a passport. Some of these original benefits depend upon widespread card-holding or compulsion. That power remains, but in 2009 the Government said it would keep card-holding entirely voluntary for all UK citizens.

1.5 The EU member states that are party to the Schengen Agreement resolved in 2004 to include fingerprint data, as well as a digital image of the face, on travel documents. The UK Government is not bound by this but has made it a policy to adopt the same level of security ('the second-biometric passport'). Biometric data on passports could offer identity verification benefits beyond those needed for travel, irrespective of identity cards, or whether the data is held centrally as well as on the travel document. The incidence of identity fraud has increased the demand for trusted identity verification and with it the need to minimise its cost, within both Government and commerce. Yet, the current political context of identity cards may deter potential users of NIS verification services from investing in changes to their systems. This reticence may extend to Government Departments given expected constraints on public expenditure.

1.6 For our final report, we offer you observations on the current priorities for the Programme to implement the NIS based on your achievements to date, the Programme's status and the context above. The Programme now needs to make benefit realisation its priority with infrastructure design and build being more closely linked to it.

---

1 the confirmation by IPS to an organisation accepting a card of its validity or its data or of the holder to the NIR record.

2. Summary of Main Observations

On Benefits & Value

2.1 Widespread card take-up, usage and realisation of benefits from this are necessary for the planned investment in the NIS infrastructure to be of value. Reliance on voluntary take-up means the creation of opportunities to use a card and the acceptance of cards for identification must be priorities of the Programme. Arrangements for card usage do not extend beyond the initial launch. The definition of, preparation for and stimulation of benefit realisation need to be incorporated into the Programme's plans.

For Citizens

2.2 Success is dependent on the citizen's perception of the value of usage opportunities. It is essential that everyday, domestic, mass-market opportunities for use be provided quickly if cardholders are not to become disenchanted. The Panel believes the consumer benefits of the card can be summarised as -

'easier for me to: identify myself; protect my identity; travel in Europe; and interact with Government'.

The most immediate of these being greater convenience than a passport for European travel.

2.3 These benefits of card-holding need to be made tangible. (3.2 - 3.5)

For Government

2.4 A combination of cost saving and service improvement for public services are sizeable potential early benefits of the NIS, subject to the necessary data governance and safeguards (2.7). The integration of all forms of identity required by all Government Departments is a natural progression of the NIS and card-holders may be perplexed if this does not take place at an early stage. More citizen-centric services, particularly self-service, will bring identity verification needs to the fore.

2.5 Cost savings from a reduction of duplication and greater standardisation of data could be substantial. We suggest that a 'store it once' policy should be adopted with a cross-Government means to make it happen. If the Government doesn't use its own Identity service, why should anyone else? (3.6 - 3.10)

2.6 Uncertainty has deterred potential identity verification service users. Hence, verification service requirements are not yet well defined. The discussions with DWP (3.5) for example may require IT-based card and address verification functions that are not yet specified in the scope of the Programme. The functionality for verification against NIR records in remote or non-face-to-face situations is a known need that is not yet specified. Definition of verification service requirements needs a high priority to inform systems design now. (3.11 - 3.17).

On Trust

2.7 Trust in the NIS is fundamental to its attractiveness. Fear of misuse of information about an individual or concerns about personal liberty threaten this. Trust requires: the record to be true; the data to be under control at all times; and the citizen to have power over its use and protections against its misuse with mechanisms for correction of errors.

2.8 The NIS must have robust data governance and operational management controls from the outset that must be institutionalised and policed to the satisfaction of the Identity Commissioner in order to provide the first two of these trust requirements. All users and all data access arrangements must adhere to these governance controls. The detailed arrangements for this should be set out. (4.1 - 4.5).

2.9 Citizen protection is to be defined by an Identity Rights Charter to be approved by the Identity Commissioner. These rights may require systems functionality that is not yet specified, as the Charter is not finalised. Finalisation and publication are urgent now that cards are in issue and systems have been commissioned. (4.3).

On Implementation

2.10 Some functions of the NIS will have greater immediate value than others. A means to value the benefits of functional releases for usage and to prioritise them accordingly is needed. (5.1 - 5.2).

2.11 The current Programme governance arrangements should be better focussed. A division of responsibilities amongst the various governance bodies would help to direct attention where it is needed. We recommend a forum responsible for strategy, involvement of interested parties, financial results and trade-off decisions (4.6), with a separate one focussed on implementation (5.13 - 5.15). The strategy board should have a director responsible for identity service specification and benefit realisation.

2.12 Programme assurance arrangements should be reviewed. (5.16 - 5.17)

3. Benefit & Value Realisation

3.1 We have noted the shift in the context of the NIS and the need to attract voluntary take-up. There are positive implications from this in the demands it places on the design.

Benefits for Cardholders

3.2 The issuance of cards in Manchester will provide further impetus to the definition of the consumer benefits of the card, which the Panel has summarised at 2.2. These need to be preferable to existing alternatives. The Panel believes that the card will be taken up by early adopters and may be well received, if the reassurances necessary for trust and the usage opportunities are in place.

European Travel

3.3 It is likely that European travel will emerge as the early leading consumer benefit. Acceptance across Europe as both a travel document and identity token needs to be assured and communicated widely.

Dealing with Government

3.4 Citizens reasonably expect Government to know what it already knows. Boundaries between different Government departments are often invisible to citizens. Progressively, card-holders are likely to be confused as to why they will also need a variety of existing forms of identification and numbers, including a driving licence and national insurance number, to do business with different parts of Government and its agencies.

3.5 Plans such as those under discussion with the DWP to make an identity card the simplest means of identification it accepts, should be pursued. The citizen would recognise real benefit in being able to interact with all parts of Government through the use of a single identifier. Without such a capability the NIS may be seen to add little more value than existing alternatives.

Benefits for Government

Combined Cost Saving and Service Improvement in Public Services

3.6 Efficiency in the provision of public services is stated as a core purpose of the NIS. In the public sector, inconsistency, variability and repetition of identity verification creates unnecessary cost and potentially is insecure for citizen and Government.

3.7 We have said that a combination of cost saving and service improvement for public services are sizeable early benefits available from the NIS, subject to the necessary trust safeguards and controls. In January 2009, the Permanent Under Secretary of State at the Home Office wrote to heads of Government Departments to seek agreement on the potential for them to use the NIS to help address this ("Safeguarding Identity - Making Services More Effective" [1]). This strategy should be followed through so that all Departments have plans to converge on the NIS as the common identifier. We suggest an approach below.

Store it Once

3.8 The Panel suggests that whilst initiatives like the DWP's "Tell Us Once" [2] are positive for citizens; alone they are add-on mechanisms for internal routing or the updating of records of several Departments. 'Tell us Once' will be difficult to achieve and maintain whilst there is a proliferation of identity databases. The strategic objective should be "Store it Once" whereby all parts of Government share the NIS as a common and definitive identity service. It may be impractical to achieve this through one major programme but it can be achieved over time if all Departments' future systems changes and enhancements are compliant with a strategic objective to use the NIS. The efficiencies possible are significant. Ancillary data that is needed only for the local Department would be held locally, alongside local applications. Some other countries, large businesses and banks operate such structures successfully. We suggest improvements to Programme management to help make this happen. (5.14).

3.9 The well-established departmentalised structure of UK Government has tended to militate against shared resources in the past. We strongly support the decision that the NIS should use the DWP's CIS biographic database. It illustrates that a 'store it once' policy is possible. Other Departments should align with this as part of 'access to Public Services' initiatives, it should be incorporated in their operational plans.

3.10 Facilitation of this alignment may identify new or changed systems requirements for the NIS. The Programme will need to be able to respond to such needs without jeopardising its progress.

---

1 http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1101.htm

2 http://www.dwp.gov.uk/newsroom/press-releases/2008/november-2008/hse113-141108.shtml

Benefits for Business

3.11 The Passport Verification Service[1](PVS) has proved popular with businesses. Few of the potential identity card verification service users have, as yet, engaged. Verification users will have current alternatives that will have a cost for them to change, although the NIS could offer a more secure and reliable alternative. Further evidence of usage benefits for the private sector needs to be developed and communicated.

3.12 Commercial verification service requirements, the business model and potential income from them are not in the NIS definition. These must be developed and inform NIS design if it is to offer a viable alternative to potential users' extant processes.

Remote Authentication

3.13 An example of the deficit in verification service requirement specifications is the lack of functionality for the anticipated need for verification against NIR records in remote or non-face-to-face situations. The role of the NIS in this should be defined, communicated and development plans made.

Define the system specifications necessary for usage

3.14 The marketing capability behind the card and NIS has been developed and the awareness campaign is well defined, with communications that are likely to appeal to the public. This will aid take up of the card. But, as usage requirements are not yet fully specified, the large-scale infrastructure that has been commissioned might require costly adaptation.

3.15 The Programme should align the user proposition, features and benefits with the infrastructure and capabilities being developed. There is a risk that these parallel tracks may diverge, rather than converge.

Lessons from the 2009/10 launch experience

3.16 A means to capture and apply lessons from the small-scale launch into the design of the full infrastructure will be needed. This should inform functional and non-functional requirement specifications and most importantly the business model and operational design of the future NIS.

3.17 The way that outputs from the new Public Panels[2] feed into NIS design requirements would benefit from greater visibility. The response to these requirements, to be benefit-driven, not infrastructure-driven, should be explicit.

4. Trust

Set out details of data governance arrangements, mandatory standards and how data will be protected

4.1 Utilisation of data by multiple users requires mandatory standards. Such standards and clear data governance arrangements that all users adhere to are essential for the integrity of the record to be trusted. The UK Border Agency's proposal to create a single Document Reader Authority (card or passport) to set standards and control the specification of readers is a practical illustration of one element of this need.

4.2 Good data governance requires a clear data model and structure, controls and authorities on change, standards of security, as well as standards of format mentioned above. Such standards and clarity of who is responsible for data, who can change it, etc., are critical and must be institutionalised. This has featured in all of the Panel's annual reports. The need for Local Authorities to adhere to security standards to access the DWP's CIS is an illustration.

4.3 The data governance arrangements and sound operational management practices must be laid out in detail, be robust and apply to all users. They should include the requirements of the proposed Identity Rights Charter.

4.4 An expert group from the Chartered Institute for IT (BCS), met with Programme management on aspects of security and counter-fraud arrangements. Topics included: the maturity of access devices; the roles of external providers in counter fraud activity; lessons from security systems elsewhere; systems integration and identity repair. A recommendation was that the Programme should adopt the BCS Personal Data Guardianship Code[3]. The Programme was to consider its own Privacy Notice to explain how it will safeguard personal data in operational practice. The Panel concur with BCS advice; the standards to be used should be published.

---

1 http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/34.htm

2 http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1189.htm

3 www.bcs.org/datacode

4.5 You have commissioned a review of IPS's bi-lateral data sharing arrangements (mostly with other Government Departments and PVS users). This should be used to design not only a standard approach but also to say how verification services will be compliant with the Act, other data statutes and the Identity Rights Charter.

Take trade-off decisions between function, security, integrity and cost at a senior level

4.6 Inevitably, trade-off decisions will arise. There is a danger that in the current financial context, compromises may weaken the integrity of the NIS, thus undermining trust, making it less attractive than alternative identification mechanisms. Management should set out the priorities and process to recognise and deal with such decisions and agree this with all the interested parties. Decisions themselves should involve all those interested, as appropriate. The Identity Commissioner and the Government's experts should be part of this process. We make observations on management process improvements that would help (5.13 - 5.17).

5. Implementation

Prioritise releases according to their benefits, and to reduce complexity

5.1 The combination of multiple suppliers, multiple Government departments and agencies both as suppliers and users, together with the sheer volume of change planned could make the schedule to build and implement the large-scale infrastructure unmanageable; particularly so as more detail of requirements is understood, is gathered from the operation launched in 2009, or is driven by benefit realisation priorities. The Panel considers this complexity is a threat to the success of the Programme, of cost escalation and delivery of the full capability.

5.2 The Programme should re-schedule and simplify releases. The Panel understands that such a review is underway. It should focus on the delivery of capabilities that enable IPS and other users to realise early benefits and to reduce risk. The re-schedule should reduce congestion that otherwise may become unmanageable. The priority for building NIS functions must be to gear cost very closely to the realisation of benefits.

Protect the simplicity of functional design

5.3 A successful NIR would be an essential component of the Government's infrastructure, supporting a wide range of users. The vast majority of its transactions would be routine and high volume such as registration, change of circumstances, etc. Some users needs, such as those of law enforcement agencies, will be less predictable, fast evolving and low volume. To satisfy both types of users within one system would potentially compromise both.

5.4 The Panel recommends that the NIR focuses on the high volume and routine processing that is possible using standard technology. To avoid compromise, more specialist needs should be separated by methods such as 'publish and subscribe', which would insulate the NIR from the complexity of the non-routine and protect the law enforcement agencies' interests from the wider community. Specialist needs should be met by applications outside the NIS.

Resist changes in requirements, give priority to benefits or simplification

5.5 There have been a significant number of requests for change (RfCs) in system requirements since supply contracts were awarded. Changing requirements increases risk, cost, timescale, or usually all three. It is essential that the RfCs be rigorously challenged to protect and ensure delivery of the core requirements.

5.6 The evaluation criteria for additional functions or changes should give priority to: benefit realisation; complexity reduction; and cost reduction. Emphasis should be given to simplicity and ease of execution. The Programme should pre-empt the complexity of multi-use that is to follow by keeping the core function as simple and straightforward as possible.

Fully resource systems integration and testing

5.7 The IPS has the responsibility for the integration and seamless operation of all the components of the NIS. Different parts, functions and operations have different suppliers and there is no prime contractor for the whole Service. The supply contracts that have been signed require suppliers to cooperate, but the penalties for failure to do so are open to legal challenge and fall short of the costs of failure of the overall system. The Programme is to establish a test and readiness centre and will employ systems-integration expertise.

5.8 The Panel noted that different suppliers use different development methodologies ('waterfall' and 'iterative' for example). At whole-Programme level there will be incremental releases as components are delivered, tested and reviewed in turn. The different approaches increase complexity and hence challenge the ability of the

Programme to deliver the whole. Management of releases or iterations will be a heavy burden with these mixed methodologies.

5.9 The test and readiness centre will be critical for successful implementation of the full-scale infrastructure. The Programme will have to employ strength in systems integration for the whole period of the build phase. The Panel has not seen how the output from tests will translate into effective change control for all of the suppliers. The change control process will have to be particularly robust and offer sufficient transparency over suppliers' milestones to provide confidence in earned value reports upon which payments to suppliers depend.

5.10 Non-functional requirements, such as response times, will be as important for satisfactory operation as the basic functions. Adequacy should be tested fully as part of integration tests as components will affect each other. The operation of biometric processes that depend on new or changed technological or security standards will require particular attention. The vagaries of human behaviour must be included in the testing process.

Closely manage operating model co-existence

5.11 IPS has established a "Transforming the Customer Experience" project to change its operating model, as the Programme is to replace existing passport infrastructure as well as add new biometric capabilities for both passports and identity cards. To create this new 'digital' operating model for the IPS and then amalgamate it with the existing passport model will be a significant challenge. This will occur during a period of expenditure constraint.

5.12 A common problem with such activity is that issues with existing operations detract resources away from the creation of the new. Clear governance measures will be needed that can prevent cannibalisation of development work to fix issues with the existing legacy. We believe that further effort may be necessary to understand what is required and the key people and assets that may be needed, if you are to run the as-is and also build the to-be. In addition, the Programme needs to review its plans to cope with the new direct relationship with service suppliers, other Government departments and UK citizens, both physically and online. Again, human behaviour must be fully accounted for in the design.

Improve the focus of NIS governance and management

Process and Responsibilities

5.13 The Programme is driven by a 'Scheme Management Board' that takes on dual functions of purpose-related decisions and operational management. This risks giving inadequate attention to both. The governance arrangements should be improved. A broader involvement of interested parties, to agree standards, increase engagement and achieve optimum trade-off decisions is needed to set strategy and priorities. The management board would then be responsible for how these 'right things' are done.

5.14 Our suggestion is to have:

a) a strategy board, responsible for: involvement, particularly other parts of Government and representation of the needs of identity verification services; the agreement of standards, priorities and trade-off decisions; benefits and financial results. This would be a more involved role than that practiced by either the 'Safeguarding Identity Strategy Group', or the 'Ministerial Identity Working Group' now, yet a wider one than that of the Scheme Management Board now;

b) a management board that would focus on delivery of the defined priorities and IPS's capabilities;

c) a documented assurance framework to inform and reassure the sponsor of delivery (5.16).

5.15 Benefit realisation and its needs should be championed at the strategy board by a dedicated directorship.

Assurance

5.16 Assurance arrangements are there to help management and to provide the sponsor with impartial confirmation that implementation is on track. The Programme has internal and NAO audit focussed on risk and control, plus periodic Gateway and Major Project Reviews by the Office of Government Commerce (OGC). The role of the newly appointed Identity Commissioner is more akin to audit (review of what has been done) than assurance.

5.17 You have decided to stand down the other assurance groups such as our Independent Assurance Panel, the Biometric Assurance Group of biometric experts and the BCS group on security. The planned Expert Group and the Identity Commissioner do not have Programme assurance roles. The Programme should now document how its assurance framework is to be coordinated to the satisfaction of the sponsor, OGC and the Identity Commissioner. This should incorporate a statement of the main risks that face the Programme and the NIS.

Capabilities

5.18 The Panel has witnessed a steady improvement in the capability of the project teams. This may not yet be sufficient for full implementation. Add to this the likely funding challenges and the Programme should:
- do fewer things: simplify the amount and range of activity, use techniques such as a 'must do', 'should do', 'could do', approach and de-prioritise accordingly;
- build greater flexibility in the IT execution team and ensure that there is organisational and resource agility;
- continue to raise IT capability, particularly in integration expertise and increase the use of support tools.

6. Conclusion

6.1 We hope our observations are useful to you and help in the development of the NIS. The most urgent is the definition of, preparation for, and stimulation of card usage, particularly by Government Departments.

6.2 The Panel has received excellent cooperation throughout, we thank you and all your colleagues for this.

6.3 The Panel has been considerably informed and assisted by the Biometric Assurance Group:
- Professor John Beddington - Government Chief Scientific Advisor
- Professor Mike Fairhurst - Head of Department of Electronics, University of Kent
- Peter Hawkes - former Assistant Director, Electronics & IT, BTG plc
- Peter Higgins - Higgins-Hermansen Group, USA
- Richard Mabbott - Director, Standards and Security at APACS
- Professor Angela Sasse - Head of Human-Centred Technology & Information Security Research Department of Computer Science, University College London
- Ing Mario Savastano - Convenor of the ISO/IEC JTC1 SC37 WG6 on "Cross-jurisdictional and societal aspects" of Biometrics and Senior Researcher at the National Research Council of Italy
- Professor Adrian Smith - Director General, Science and Research in DIUS
- Philip Statham- Former Biometrics Programme Manager, CESG & Chair, Government Biometrics Working Group
- Dr Valorie Valencia - Chief Executive Officer of Authenti-Corp and Research Professor of Optical Sciences at the University of Arizona

6.4 We are very grateful for the wise council Mr Bob Assirati Major Projects Director at Office of Government Commerce and Deputy President of the Chartered Institute for IT (BCS).

The Panel

6.5 Members of the Panel, to whom I am greatly indebted, have been:

- John Clarke, a Senior Vice President and Chief Information Officer of Nokia Corporation;

- Malcolm Mitchell, an independent IT consultant, previously held IT leadership roles in Glaxo, Glaxo Welcome, Vodafone and BAA;

- Peter Simpson, a strategic marketer with a wide consultancy and executive portfolio, with considerable experience in proposition development and communications;

- Fergie Williams has forty years experience of delivering large scale IT dependent change, including identity management in retail banking. He has worked in Asia, North America and Europe, most recently as Chief Information Officer of HSBC Europe.

Alan Hughes 17 December 2009